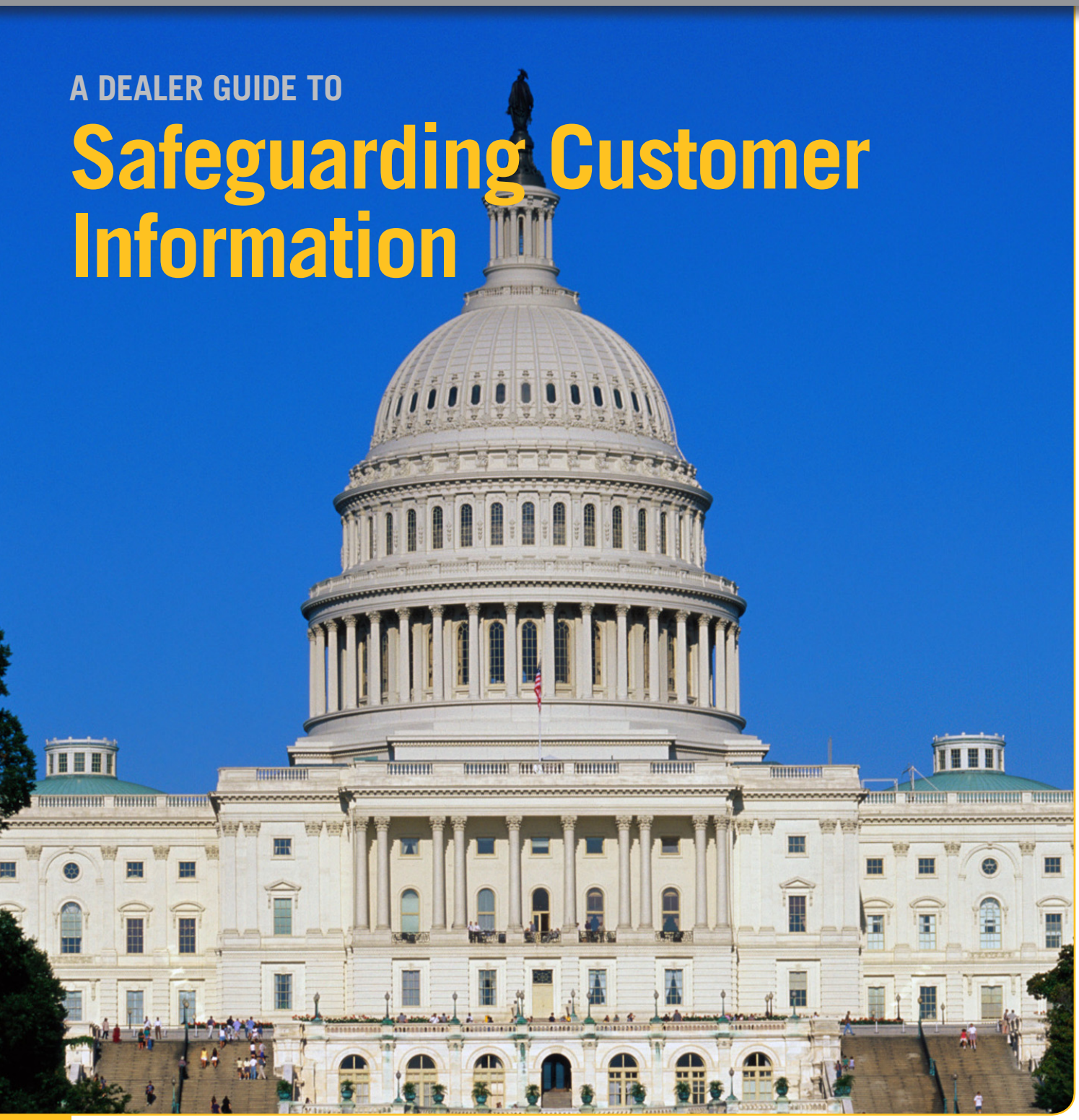
Driven

L43

NADA MANAGEMENT SERIES

A DEALER GUIDE TO

Safeguarding Customer Information



L43

NADA-ATD Resource Toolbox

PREFACE

The purpose of this management guide is twofold. First, it explains a new Federal Trade Commission rule that requires automobile dealers to develop, implement and maintain a comprehensive written Information Security Program to protect the dealership's Customer Information. The guide provides an overview of the new requirements and then discusses in detail each of the five main elements that the program must contain. Second, it provides at Appendix A a sample template to assist dealers in preparing their Information Security Program. The appendixes also contain other useful information, including sample language for employees to acknowledge their information safeguarding obligations (Appendix F) and sample information safeguarding clauses to use in your contracts with service providers that have access to your Customer Information (Appendix J).

Dealers must be in full compliance with the requirement to have an Information Security Program in place by May 23, 2003.

Nothing in this guide (including the appendixes) is intended as legal advice. The requirements of this rule and the varied circumstances of each dealership are too complex to simply mechanically adopt the sample Information Security Program at Appendix A (or the language at Appendixes F and J). In addition, this guide only discusses the federal Customer Information Safeguarding Rule. It does not discuss state or local law that may impose additional requirements. It is essential that you draft a written Information Security Program that is appropriate to your dealership and that you have it reviewed by qualified legal counsel.

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.

Paul D. Metrey
Director, Regulatory Affairs
February 2003

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

A Dealer Guide to Safeguarding Customer Information

Table of Contents

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

A Dealer Guide to Safeguarding Customer Information

I. INTRODUCTION

By now, all dealers are familiar with the requirements of Section 501(a) of the Gramm-Leach-Bliley Act (GLB) and the Federal Trade Commission's (FTC) privacy rule (Privacy Rule),[1] obligating them to disclose to their finance, lease and insurance customers how they use and share consumer information. Now the FTC has published a new rule that is in addition to, and independent of, the Privacy Rule. It is the FTC's "Standards for Safeguarding Customer Information" (Safeguards Rule).[2] **The Safeguards Rule requires dealers to develop, implement and maintain a comprehensive written information security program. It also requires dealers to ensure their affiliates maintain appropriate safeguards, and dealers must select and retain service providers that are capable of maintaining appropriate safeguards, for the customer information dealers share with them**. The final compliance date for the Privacy Rule was July 1, 2001. **The final compliance date for the Safeguards Rule is May 23, 2003.**

The intended purpose of GLB is twofold. First, it hopes to raise consumers' awareness of the different ways their "nonpublic personal information" may be used by requiring dealers who engage in financial transactions with consumers to provide privacy notices outlining their information sharing practices.[3] The Privacy Rule implements this purpose. Second, it seeks to protect the financial institutions' customers from identity theft and other harm by requiring financial institutions to assess their data and information controls and take steps to protect customer information from misappropriation, alteration, tampering, etc.[4] The Safeguards Rule implements this purpose.

You can distinguish the Privacy Rule from the Safeguards Rule as follows:

- The Privacy Rule deals with how you *share* information about consumers who obtain, or apply for, credit or lease products from you.

- The Safeguards Rule deals with how you *protect* information about your finance and lease customers, regardless of whether you sell the obligation to a third party finance company or lessor.

These obligations, while related, are independent of each other and subject to different standards, so you will need to be careful that you take appropriate steps to comply with each. 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.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

You should know that the Safeguards Rule is not a new concept – it was mandated by GLB,[5] and the FTC has now complied with that mandate. In fact, you may recall that the Privacy Rule contemplates this new Safeguards Rule, in that the Privacy Rule requires you to make a statement about your information safeguarding practices in your privacy notices.[6] Indeed, the Privacy Rule provides the following "model" language for your privacy notices: "*we maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information*."[7] The Safeguards Rule is the "federal regulation" to which this model language refers.

This Guide will explain the Safeguards Rule and your obligations as automobile dealers to comply with it. Given the advent of the Internet and numerous data management tools, 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 dealer's perspective, there is also the potential liability arising out of customer information getting into the wrong hands. Therefore, while the Safeguards Rule applies specifically to the personal information of your finance and lease customers, the protections it affords may be just as relevant to all of your customer data, including sales, service and parts data.

The purpose of this Guide is to familiarize you with your obligations under the Safeguards Rule. Right now, it is unlikely that your dealership has a formal Information Security Program in place. Accordingly, much of the information in this Guide will be new, and perhaps, overwhelming. Nevertheless, the Safeguards Rule is a reality, and your compliance is required no later than May 23, 2003. Fortunately, the FTC (the federal agency that enforces the Safeguards Rule) realizes that a "one-size-fits-all" rule is unworkable, and has granted you a fair amount of flexibility in how you comply.

The Sample Information Security Program at **Appendix A** is designed to be a starting point from which you can develop your own Information Security Program, that is, one that addresses the information security matters specific to your dealership. **It 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 Information Security Program. Because each dealer'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.

Finally, please note that **this 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 will be developed by your state's Insurance Department. In addition, the individual states (and perhaps, some localities) may impose even more stringent safeguarding standards, making it even more important that you work with your legal counsel to ensure that your Information Security Program meets the standards of any applicable state or local laws.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

II. OVERVIEW OF THE SAFEGUARDS RULE

A. Applicability of the Safeguards Rule

Which dealers are covered by the Safeguards Rule?

The Safeguards Rule applies to all dealers who are "financial institutions" under GLB and the Privacy Rule. In other words, any dealer that is "significantly engaged in financial activities" is a financial institution.[8] "Financial activities" include such things as entering into finance or lease transactions with consumers.[9] It also includes insurance transactions, but those are governed by rules set by your State Insurance Commissioner.[10]

The FTC has never defined the phrase, "significantly engaged," but as a rule of thumb, you should consider yourself "significantly engaged" in financial activities for purposes of the Safeguards Rule if you regularly provide installment sale and/or lease financing to consumers, even if you immediately assign sale and lease contracts to a bank or finance company.

Applicability of the Rule to Medium- and Heavy-duty Truck Dealers

The Safeguards Rule, like the Privacy Rule, applies only to transactions involving natural persons who obtain a financial product or service from you primarily for personal, family, or household purposes.[11] It does not apply to information about companies or about individuals who obtain financial products or services for business, commerical, or agricultural purposes.[12] Therefore, to the extent your financing activities are primarily for one of these latter purposes, the Safeguards Rule does not apply. This would probably be true for most medium and heavy-duty truck dealers. Likewise, the Safeguards Rule would be unlikely to apply to wholesale transactions for automobiles to the extent the financing is between you and a business or other entity, e.g., not a natural person (transactions with sole proprietors acting in a business capacity also would not be covered).

What information is covered by the Safeguards Rule?

The Safeguards Rule requires you to adequately protect and safeguard "Customer Information."[13] Customer Information is "any record containing 'nonpublic personal information' as defined [in the Privacy Rule], 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."[14]

In general, Customer Information is information about a consumer with whom you have entered into a finance or lease transaction, for example, information contained in a consumer's credit report or credit application, account numbers, bank balances, etc. It includes not only information about your customers **but also information you receive about the customers of other financial institutions** (e.g., banks, finance companies, other dealerships, etc.).[15] Even lists of the names of your finance or lease customers would be covered by the Safeguards Rule.[16] Note that for purposes of the Safeguards Rule, Customer Information does **not** include information you obtain from potential finance or lease customers – only Customer Information relating to actual customers is covered.

An important note here – while Customer Information includes information related to insurance transactions, the Safeguards Rule does not apply to such information. That is because GLB requires each state Insurance Department to issue its own safeguards rule with respect to customer information relevant to insurance transactions.

Because it is so difficult to separate Customer Information that is part of a finance or lease transaction from that which is part of an insurance transaction, it would be prudent to apply the Safeguards Rule protections to all insurance-related customer information. In fact, as discussed below, it may be prudent to apply such protections to all of your customer data.

You should work with your legal counsel to determine whether there are any data protection laws in your state with which you must also comply. For example, GLB requires each state to issue a safeguards rule applicable to insurance transactions, and it is possible that your Insurance Commissioner will issue a safeguards rule that is more stringent than the FTC's Safeguards Rule. Your state may have other data protection laws applicable to your business, such as a law requiring you to notify any consumers if their personal information is violated in any way, so you will need to develop a means to identify such laws and a means to stay abreast of new laws as they may arise.

As noted above, you may find that it would be difficult and/or expensive to try to separate protected Customer Information from other information for safeguarding purposes. For example, the Privacy Rule distinguishes between *consumers* and *customers*[17], the latter being a subset of the former, and provides different protections for each. Despite this, many dealers give their privacy notices to all of their consumers, even though they technically may not be required to do so.

While the Safeguards Rule applies only to Customer Information as defined above (including information about *former* customers), you may find it prudent to subject all of your data about consumers to the protections of the Safeguards Rule. This approach will go a long way towards ensuring the safety and security of such data, and provide a real service to your entire customer base. For example, a service customer who pays for repairs with a personal check could just as easily be a target for identity theft as a finance or lease customer, particularly if it is your practice to write the customer's driver's license number on the check. The same is true of a consumer who completed a credit application, but then decided to pay cash for his or her vehicle.

When is the Safeguards Rule effective?
You must implement an Information Security Program no later than May 23, 2003.

B. Safeguards Rule Requirements

A comprehensive, written Information Security Program
The Safeguards Rule requires you to develop, implement and maintain a comprehensive, written Information Security Program. It also requires you to ensure that your affiliates maintain appropriate safeguards and your service providers are capable of maintaining appropriate safeguards for the Customer Information you share with them.

Your Information Security program will be a written document 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. Your Information Security Program may be contained in one or more documents. For example, that part of your Program applicable to employee training and management could be contained in your dealership's policies and procedures relating to employees.

Program objectives

GLB and the Safeguards Rule require that your Information Security Program meet these three objectives:

- Insure 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.

Five required elements

The Safeguards Rule requires that the following five elements be included in your Information Security Program. Each element is discussed in detail in the next section entitled "A Step-By-Step Guide to Developing, Implementing and Maintaining Your Information Security Program." All of these elements, except the first element (designating an employee to coordinate the Information Security Program), may be outsourced at your discretion. Your Program Coordinator must oversee your outsourcing contractors to ensure the functions they are to perform are properly carried out.[18] You will want to interview and check the references of any potential vendors to determine whether they are appropriate for your situation. Also, you must have a contractual agreement with your vendors requiring them to keep any Customer Information they have access to or otherwise come across confidential, and to have safeguards in place themselves that are adequate to protect your Customer Information.

1. You must designate an employee or employees (Program Coordinator(s)) to coordinate your Information Security Program.

2. You must 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 consider risks in each area of your operations (risk assessment process). Three areas requiring special consideration are:

   - Employee training and management;
   - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
   - Detecting, preventing and responding to attacks or intrusions on your electronic and non-electronic information systems, or other information systems failures.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

3. You must design and implement Customer Information safeguards to control the risks you identify through the risk assessment, and regularly audit the safeguards to ensure their effectiveness.

4. You must oversee service providers by:

   - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for your Customer Information; and
   - Requiring your service providers by contract to implement and maintain such safeguards.

5. You must evaluate and adjust your Information Security Program in light of:

   - The results of your audits;
   - Any material changes to your operations or business arrangements;
   - Any changes in widely available technology; or
   - Any other circumstances that you know or have reason to know may have a material impact on your Information Security Program, including, any changes to equipment, applications and services provided by your service providers.

Compliance standards

The FTC tried to fashion the Safeguards Rule's requirements to be as ***flexible*** as possible, yet still consistent with the purposes of GLB.[19] Under the FTC's "flexible" standard, your safeguards must be appropriate to:

- The size and complexity of your dealership (or family of dealerships) and its operations;
- The nature and scope of your dealership's (or family of dealerships') finance and lease activities; and
- The sensitivity of the Customer Information you collect, store, transmit, etc.

While there may be similarities between the Information Security Programs each dealership or family of dealerships implements, the fact is that the Programs will contain significant differences. This "flexible" standard should permit dealerships, in particular smaller dealerships, to simplify their Information Security Programs to the same extent their overall operations are simplified. This does not mean to say that enforcement will be flexible, rather, the FTC will look at the three prongs of its flexibility standard (above) to determine whether a particular dealership is in compliance.

You can look at the "flexible" standard this way:

- Your safeguards will be proportionate to the size and complexity of your operations. Greater size and complexity typically mean more opportunities for information misappropriation, data corruption, hardware/software problems, etc.

- In general, the more finance and lease transactions you enter into, the greater the likelihood you will need to put more thorough safeguards in place.
- The Customer Information you acquire in finance or lease transactions is among the most sensitive information you receive. You will want to consider this as you design and implement your Information Security Program.

At the end of the day, your compliance obligations under the Safeguards Rule are subjective at best. There is no articulated "minimum compliance" standard, e.g., there is nothing that says, "If you do X, Y and Z, you will be in compliance." Each dealership will have different obligations based on the three-pronged flexibility standard.

Example: You are a small dealership. Your F&I manager works alone, and routinely leaves the paper credit applications taken that day on her desk. A number of different customers or vendors come through her office during the day, and can view these applications. What safeguards should you consider?

In this case, it would be appropriate to require your F&I manager to keep credit applications and other sensitive customer data in a locked drawer or cabinet. At the very least, such data should be kept in folders, to be securely filed later in the day. In addition, customers and vendors should not be left in the office unsupervised unless the data is secured. The door to the office should be locked when it is unattended. Also, even when the F&I manager is in her office, the paper credit applications should not be left in plain view of anyone not authorized to have access to Customer Information.

Example: You are a large, multi-franchise dealership. You have a large database of customer information, including vehicle information, finance or lease information, service history, follow-up information, etc. Any employee in the dealership may access this information, from the F&I Department to the Service Department, to the receptionist. In addition, your manufacturers can also access your database remotely to pull the information they require from time to time. What safeguards should you consider?

Here, more sophisticated safeguards are called for than in the prior example. Some of these may be:

- *Use passwords to limit access to the database, that is, limit access based on an individual's need for it under his or her job description. Only persons with a true "need to know" finance and lease data should be granted access to such sensitive information. Service personnel and clerical staff are not likely to need to access this data, and this should be reflected in their password security level.*
- *The database should be password protected as to the manufacturer as well. A manufacturer is, in most instances, a "non-affiliated third party" under GLB, and is generally not entitled to obtain GLB-protected consumer/customer information from you unless (i) one of the Privacy*

Rule exceptions to the opt out requirement applies,[20] or (ii) your consumers/customers have not "opted-out" of such sharing after having been provided the opportunity to do so.[21] If neither has occurred, the manufacturer should be blocked from viewing personal consumer information relating to the consumer's actual or proposed finance or lease transaction.

- *Computer servers containing your customer databases should be housed in climate-controlled, controlled-access rooms, and should not be accessible through the Internet. In addition, up-to-date firewalls and anti-virus protection should be used.*

Penalties for not complying with the Safeguards Rule

The penalties for not complying with the Safeguards Rule are identical to those for not complying with the Privacy Rule. In the case of automobile dealers, the FTC can initiate an enforcement action against you under the authority granted to them in the Federal Trade Commission Act, 15 U.S.C. § 41 *et seq*.[22] Penalties may include monetary fines, injunctive relief and long-term consent decrees.

The Safeguards Rule does not permit an individual (or a class of individuals) to bring a lawsuit against you for violating the Safeguards 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. 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. 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.

As you read through the following suggestions, you will undoubtedly be struck by how considerable an undertaking it is to comply with the Safeguards Rule. For example, the amount of effort involved in performing a risk assessment, developing and implementing appropriate safeguards, and monitoring and auditing your safeguards, though directly related to the size, nature and complexity of your operations, is substantial. While large dealer organizations are likely to have a number of human resources involved in the compliance effort, redirecting even one or two individuals in a smaller dealership can have a significant impact on the business. Even so, the Safeguards Rule requires that you develop, implement and maintain a comprehensive written Information Security Program, regardless of its impact on your day-to-day operations.

Additionally, despite the FTC's "flexible" standard, compliance will be ongoing and may be expensive. For those of you with sophisticated computer systems and information management tools (e.g., DMS, F&I, CRM and business partners who host call centers and websites), it is likely you will need to turn to outside help in order to accomplish the tasks required of you under the Safeguards Rule. Even if your systems are not state-of-the-art, you will probably need some outside assistance to help you determine the potential risks to your Customer Information and the

appropriate fixes. In most, if not all, cases, you will need to revisit your budget to ensure that adequate funds will be available to meet your compliance obligations on an ongoing basis.

As you review the following, keep in mind that the actual steps you take must be consistent with your individual operations. A large and complex dealership operation will more than likely violate the Safeguards Rule if its compliance efforts are limited to those a smaller and less complicated operation would undertake. Likewise, smaller and less sophisticated dealerships probably will not need to go to the lengths large dealership organizations will in order to achieve compliance.

III. A STEP-BY-STEP GUIDE TO DEVELOPING, IMPLEMENTING, AND MAINTAINING YOUR INFORMATION SECURITY PROGRAM

A. Designating an Information Security Program Coordinator

What are the initial and ongoing responsibilities of the Program Coordinator?
Your Program Coordinator will be responsible for coordinating your Information Security Program across your dealership or family of dealerships. He or she will manage your compliance obligations under the Safeguards Rule.

Your Program Coordinator should be familiar with all areas of your operations. Because of the ongoing compliance requirements the Safeguards Rule imposes, such as testing and monitoring, you may want to designate a principal, or other long tenured person, as your Program Coordinator. He or she may find it necessary to rely on persons in different areas of your operations for advice and assistance in order to adequately fulfill his or her duties under the Safeguards Rule. In addition, it is highly likely that the Program Coordinator will need to turn to outside sources for guidance in complying with the Safeguards Rule and performing his or her functions under it. The Safeguards Rule permits the Program Coordinator to delegate or outsource the safeguards functions, provided the Program Coordinator ensures that those functions are properly carried out. The Program Coordinator cannot, however, outsource his or her position. *The Program Coordinator must be an employee of your dealership.*

Your Program Coordinator must be empowered with the ability and resources to design, implement, maintain and enforce the safeguards he or she deems necessary. That is, the Program Coordinator must oversee

- The Safeguards Rule's risk assessment requirements;
- The development, implementation and maintenance of your written Information Security Program;
- Vendor relationships to ensure that they are in compliance with the Safeguards Rule; and
- The Safeguards Rule's audit and monitoring requirements.

The Program Coordinator must have the authority to enforce your safeguards, and take action when necessary to deal with threats to the security or integrity of your Customer Information.

Will my Program Coordinator be subject to personal liability in the event my dealership does not adequately comply with the Safeguards Rule?
In general, the answer to this question is no. Your Program Coordinator will not be subject to any more liability than any other employee of the dealership.

The Safeguards Rule does not address or alter traditional principles of entity liability and, therefore, should neither create nor limit individual liability for your Program Coordinator. What this means is that there is nothing in the Safeguards Rule that could, on its own, be the direct basis for a claim against your Program Coordinator. Traditional liability principles tend to hold the employer liable for the wrongful acts of the employee, except when the employee has acted outside the scope of his or her employment. So, the liability risks already facing your employees exist unaltered by the Safeguards Rule. For example, if your Coordinator were to misappropriate Customer Information, he or she could be subject to civil and criminal liability, e.g., liability for identity theft, fraud, etc. The Safeguards Rule has not changed this. Your Program Coordinator could not be held directly liable under the Safeguards Rule for a failure in your information safeguards. However, the dealership could be held liable (see the Penalties discussion on page 10).

How many Program Coordinators must I designate?
The actual number is up to you and will depend on the size and nature of your operations. However, each dealership must have its own Information Security Program and at least one employee who is designated as the Program Coordinator.

If you operate multiple dealerships and your operations are large and centralized, you may want to designate employees from different departments, e.g., F&I, Sales, Service, Human Resources, Legal, Marketing, to assist your Program Coordinator(s) with overseeing the program functions. It also may be prudent to designate one managing Program Coordinator to work with the designated Program Coordinators in each dealership to coordinate their Information Security Programs. Although each dealership must have its own Program Coordinator and Information Security Program, the dealerships within your family of companies may share many Information Security Program functions, such as using the same third party for document disposal services. Ultimately, how you execute the program functions will depend on the organizational structure and operations of your dealership.

The FTC is particularly concerned that small operators not be burdened disproportionately by this requirement or the Safeguards Rule generally, and has tried to achieve a balance between the objectives of the Safeguards Rule and the realities of business. Therefore, you are empowered to determine which, and how many, employee(s) to designate, including whether to designate additional employees to handle different subsidiaries or areas of your operations.

From which areas of my operations should my Program Coordinator come?
Again, this will depend on the size and nature of your operations. Smaller dealerships are likely to appoint a single Program Coordinator. Large dealer groups are likely to appoint several Program Coordinators (specifying one of them to chair the Committee of Coordinators) from different areas of their operations, for example:

- Finance and Insurance
- Sales
- Service
- Parts
- Accounting
- Information Technology/Systems

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- Marketing
- Risk Management
- Human Resources
- Legal
- Each Dealership

You will have to be the judge of what makes the most sense in the context of the FTC's three-pronged flexibility standard (e.g., the size and complexity of your dealership(s) and its operations, the nature and scope of your finance and lease activities, and the sensitivity of the Customer Information you collect, store, transmit, etc.).

To whom should the Program Coordinator report?
The Safeguards Rule is almost identical to the safeguarding rule with which banks, thrifts, and other more traditional financial institutions must comply (Bank Rule). One major difference between the Safeguarding Rule and the Bank Rule is that the Bank Rule requires that the Coordinator(s) involve and report to the bank's Board of Directors.[23]

To the extent your dealership is a corporate entity with a board of directors, it would be prudent to follow the Bank Rule requirement, e.g., your Board of Directors should be involved, and should require regular reports from your Program Coordinator. To the extent your dealership is organized differently, e.g., as a partnership, limited liability company, etc., your Program Coordinator should involve, and report to, senior management. To the extent you are a sole proprietorship, you may choose to be the Program Coordinator yourself.

The purpose of such high-level involvement and reporting is twofold. First, it places responsibility for data protection where it should be – at the top. Second, the involvement of senior management and/or the directors makes it easier for the Program Coordinator to perform his or her obligations under the Safeguards Rule. Cooperation in the ranks is more easily achieved when everyone knows that the Program Coordinator is acting at the request of senior management.

How long must I keep my Program Coordinator in place?
The role and duties of the Program Coordinator are ongoing, so you are required to keep the position filled on a permanent basis. Of course, you can replace your Program Coordinator as necessary, but it would make sense to have a procedure in place to facilitate a smooth transition.

B. Risk Assessment

The Safeguards Rule requires that you:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of your Customer Information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise; and
- Assess the sufficiency of any safeguards you have in place to control these risks.

As you may recall from NADA's "A Guide to the FTC's Financial Privacy Regulation" (the guide explaining the Privacy Rule), we suggested that you conduct a "privacy audit" in order to discover all instances in which you may disclose nonpublic personal information to third parties. Doing so was a good way for you to determine how information was shared with your affiliates and non-affiliated third parties so that you could determine what your information sharing policies would be and draft an accurate privacy notice. Indeed, you should conduct periodic privacy audits to ensure your continued compliance with the Privacy Rule.

Under the Safeguards Rule, conducting a risk assessment in your dealership is not an option — it is a requirement. This fact is evidence of how important Congress and the regulatory agencies feel about the Safeguards Rule's intended purpose, that is, to protect against identity theft and other harm that may befall a consumer whose personal information finds its way into the wrong hands.

What are the objectives of performing a risk assessment?
The point of your risk assessment is to determine those areas of your operations where there is a "reasonably foreseeable" risk that your Customer Information may be compromised. "Reasonably foreseeable" is a very general term, and by using it, the Safeguards Rule recognizes that the threats to information security are ever changing. "Reasonably foreseeable" threats can be different for different dealers. See **Appendix C** for some examples.

What areas of your operations should be included in your risk assessment?
The Safeguards Rule requires that your risk assessment cover "all relevant areas" of your operations. At a minimum, you must pay special attention to:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to attacks and intrusions on your electronic and non-electronic information systems, or other systems failures.

For many of you, it may be sufficient to focus on the three operational areas noted above. However, the larger and more complex your operations are, the more likely it is that other areas should be reviewed in the course of your risk assessment. For example:

- You need to review your vendor and service provider relationships, e.g., third party finance/lease software vendor, offsite storage facilities, call centers, to the extent such third parties perform tasks that may require or permit them to access Customer Information. This also is required to fulfill the fifth element of your Information Security Program (Overseeing Service Providers), which is discussed in detail later in this guide.
- If you are using the same database to track your finance and lease customers as you are for your cash and service customers, you should extend your training to your service staff and others who may have reason to access the database.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- If your sales staff maintains databases or lists of Customer Information for their own use, or otherwise have reason to access Customer Information, you should extend training to your sales staff.

As you conduct your risk assessment, be sure to remember that it must address threats to all of your Customer Information in whatever form, e.g., paper, electronic, etc. Your risk assessment should also cover Customer Information wherever it is, be it in an office, on a computer server, at an offsite storage facility or the trunk of your employee's car.

1. Risk Assessment -- Employee Training and Management

What kind of employee training is necessary, and which employees should be trained?

Any employees that have access to Customer Information should receive some kind of safeguards training. Ideally, you should think about training all of your employees and independent contractors, because your safeguarding obligations cover your entire enterprise. While minimal, periodic training may be sufficient for reception staff, mechanics and other service personnel, and others whose responsibilities do not require them to have access to Customer Information, you should undertake more comprehensive training for your F&I department, bookkeeping and accounting staff and other staff, including independent contractors, whose jobs require them to access Customer Information.

The term **"independent contractor"** is not defined under the Safeguards Rule. Independent contractors are, however, "service providers," if they receive, maintain, process or otherwise are permitted access to Customer Information through their provision of services directly to a dealership. Thus, you must ensure that you comply with the Information Security Program requirements applicable to your service provider relationships when entering into and maintaining relationships with independent contractors. If an independent contractor will have access to Customer Information and will be **performing services in your dealership**, it would be prudent to ensure that the independent contractor receives the same Information Security Program training that an employee with the same access to Customer Information would receive.

How often must employees be trained on information security procedures?

The Safeguards Rule does not address the frequency of training, and leaves it to the judgment of each individual dealership (or corporate family of dealerships). However, it would be a "best practice" for all new employees/independent contractors to receive safeguards training during their orientation, and for all employees to receive periodic training. The frequency of follow-up training will depend on the nature and complexity of your activities, but should occur no less than once each year.

What are management's responsibilities with regard to employees and the safeguarding of Customer Information?

Your Information Security Program will contain, at the very least, your policies and procedures regarding employee training and management, information systems, and preventing attacks, intrusions and other acts that could compromise Customer Information. In effect, much of it could double as an "employee manual" of sorts,

except to the extent it contains information unsuitable for broad distribution, for example, documentation regarding electronic protections you may have in place (e.g., firewalls), your criteria for vendor selection, etc.

Management should maintain its traditional role with respect to Safeguards Rule compliance and enforcement. That is, while the Program Coordinator has overall responsibility, management should provide any assistance necessary to ensure that your staff receives the appropriate training, and that your Information Security Program is followed. In the event that you become subject to an enforcement action or other litigation or investigation, it will be important that you be able to show that your Information Security Program complies with the Safeguards Rule, and that you have procedures in place to ensure your dealership's compliance with each element of your Information Security Program. Most importantly, you will want to be able to document your employees' violations of your Information Security Program, and how the responsible employees were disciplined.

How do you determine whether your current procedures relating to employee training and management meet the requirements of the Rule?
In this portion of your risk assessment, your object is to determine what dangers exist to the security and confidentiality of your Customer Information in the context of your employee management and training policies and procedures.

- Review your operations and identify any "reasonably foreseeable" risks to Customer Information.
- Identify your current employee training and management policies and procedures.
- Conduct a critical review of your current employee training and management policies and procedures and determine whether they sufficiently mitigate the potential risks you have identified. Look at the FTC suggestions outlined in **Appendix E** for guidance on appropriate employee training and management.
- If your current employee training and management policies and procedures sufficiently mitigate the risks you have identified, then they should be included "as-is" in your comprehensive written Information Security Program.
- If your current employee training and management policies and procedures do not sufficiently mitigate the risks you have identified, your Program Coordinator should design new policies and procedures that do, and include them in your comprehensive written Information Security Program.
- In either event, you will need to work with your Program Coordinator to ensure that your employee training and management policies and procedures are appropriately implemented and maintained. This includes modifying these policies and procedures over time as changes to your operations or technology may require.

What safeguards should you consider?

- Limiting access to Customer Information to those employees with a need to know it.
- Providing guidelines for choosing vendors who may have access to Customer Information. (See the Q&A at page 27 entitled "What qualifies as reasonable steps to use when selecting or determining whether to retain service providers?")

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- Locking file cabinets, as well as the rooms where Customer Information is received, used or stored.
- Locking rooms containing computer servers that contain Customer Information.
- Using secure off-site storage facilities.
- Using strong passwords (e.g., alpha-numeric, at least 8 characters long).
- Using password protected screensavers on terminals from which Customer Information is accessed, and/or for computer programs that access Customer Information (credit applications, credit reports, etc.).
- Prohibiting the use of passwords by anyone other than the individual to whom it belongs.
- Immediately closing down access to Customer Information for employees who cease working for the dealership, including deleting their passwords.
- Disciplining employees for violations of your Information Security Program, up to and including termination.

You may wish to develop a checklist for determining whether current and future employee management and training procedures are adequate. Since each dealer's operations are unique, it is not possible to provide a checklist that would provide you with the level of detail needed to review your unique training procedures for the various levels of employees who may have access to Customer Information. You may, however, use the sample checklist provided at **Appendix D** as a starting point from which you can develop your own comprehensive checklist. **It is not intended to be a turnkey product that you can simply adopt as your own.**

2. Risk Assessment -- Information Systems

This part of the Safeguards Rule requires you to review and revise your procedures relating to your information systems (both electronic and non-electronic), including network and software design, as well as information processing, storage, transmission and disposal.

What are "information systems" for purposes of the Safeguards Rule? Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. This would include:

- Your DMS systems
- Your paper files
- Your dealership's computer network, including computer terminals, servers, etc.
- Personal Digital Assistants, e.g. PalmPilots or other handheld devices (PDAs)
- Third party F&I software and systems
- Firewalls
- Doors and filing cabinets
- Internet access
- Record disposal policies

Identify reasonably foreseeable risks

In your efforts to identify the reasonably foreseeable risks to your Customer Information, you should think about the questions below in the context of both paper and electronic Customer Information, and in the context of internal as well as external uses (e.g., within the dealership and with respect to services provided or hosted by third parties).

- How is your Customer Information accessed?
  - Internet?
  - Computer terminal?
  - DMS?
  - PDA?
  - Paper files?
  - Modem dial-in?
  - Third party software or platform?

- How is your Customer Information collected?
  - Service advisor?
  - Call center staff?
  - Internet?
  - Email?
  - Telephone?
  - Paper?
  - Third parties?
  - Salespersons?
  - F&I staff?
  - Other personnel?
  - Third party software or platform?

- How is your Customer Information distributed?
  - Private networks?
  - VSAT?
  - Internet?
  - Email?
  - Fax?
  - Third party software or platform?
  - DMS?
  - Mail service?
  - Courier service?
  - Dealership-wide?
  - "Need to know"?

- How is your Customer Information processed?
  - Third party software or platform?
  - DMS?
  - F&I staff?
  - Other personnel?

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- How is your Customer Information stored?
  - File cabinet?
  - Computer servers?
  - PC hard drives?
  - Laptops?
  - Floppy disks/CD-ROMs?
  - Off-site storage?

- How is your Customer Information used?
  - F&I functions?
  - Marketing/Remarketing?
  - Customer service?
  - Service/Parts department?

- How is your Customer Information transmitted?
  - Private networks?
  - VSAT?
  - Internet?
  - Email?
  - Telephone/Fax?
  - Wireless technology?
  - Mail service?
  - Courier service?
  - Third parties?
  - Salespersons?
  - F&I staff?
  - Other personnel?
  - Third party software or platform?

- How is your Customer Information disposed of?
  - Communal waste bins?
  - Dedicated/Secure disposal bins?
  - Shredders?
  - Disposal companies/Other third party vendors?
  - Reformat hard drives/Floppy disks/CD-ROMs?
  - Destroy outdated hardware/software?

- How else does your Customer Information interact with your information systems?

Be sure to tailor your risk assessment to your specific operations. Even if you manage Customer Information in ways not covered above, you are still responsible for safeguarding such information in accordance with the Safeguards Rule.

Audit your current safeguards

Once you have identified the reasonably foreseeable risks to your Customer Information, you need to inventory your current safeguards. While each dealership will have different safeguards in place, the following is a list of some you may have:

- Policies requiring employees to protect Customer Information

- Safeguards training for employees
- Limited access to Customer Information
- Password protected computers
- Door and file cabinet locks
- Document shredders
- Secure waste bins
- Firewalls
- Encryption technology
- Limitations or prohibitions on the transmission of Customer Information via wireless technology

Assess the adequacy of your safeguards in relation to the risks you identify
After identifying your reasonably foreseeable risks to your Customer Information and inventorying your current safeguards, you will need to compare your risks to your safeguards and determine whether your current safeguards are adequate (relative to the risks you face), or whether you need to design and implement new safeguards.

You must decide what safeguards are appropriate for your dealership. You may do this on your own, you may do it with the assistance of your CPA, legal counsel and/or third party vendors, or you may outsource the responsibility (subject, of course, to oversight by your Program Coordinator). Because each dealer's operations will be different, it is impractical to give you a list of safeguards "guaranteed" to meet FTC standards. However, we have provided a list of "good" practices and "risky" practices at **Appendix G**. Keep in mind that the good practices may not be suitable for your operations. You must tailor your safeguarding practices to meet the objectives of the Safeguards Rule in the context of your operations.

We also have set forth at **Appendix H** suggestions on how to safeguard your information systems throughout the life cycle of Customer Information (that is, from collection to disposal) based on suggestions issued by the FTC.

Question: Is it permissible under the Safeguards Rule to continue transmitting customer applications for financing via facsimile to a third-party bank or finance company with whom you have a contractual relationship? What about sending the same information over the Internet?

As discussed in Appendix H, you should, at a minimum, use currently accepted security standards for transmitting Customer Information in any manner to any source. Although not specifically addressed by the FTC's Safeguards Rule, transmitting such information by facsimile appears reasonable at the present time. Of course, you should ensure that the credit application does not lay around the fax machine unattended and you should ensure the application was successfully transmitted to the appropriate person at the bank or finance company. It may be prudent to preprogram your fax machine so that users may simply push one button to transmit applications to your financing sources. This should minimize input errors that would result in such information being transmitted to an unintended source.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

The same considerations apply to the transmission of customer credit applications over the Internet. You should ensure that the program application you use encrypts the data or otherwise transmits it in a secure manner to the bank or finance company. If you are submitting the customer's application over the Internet, you should ensure that the information displayed on your computer screen is not visible to others who are not authorized to have access to this information.

Regardless of the means of transmission, you also must ensure the disclosure of the Customer Information complies with your obligations under the FTC's Privacy Rule, the Fair Credit Reporting Act, any applicable requirements under state or local law, and the statements contained in your privacy notices.

3. Risk Assessment -- Managing Systems Failures

This part of the Safeguards Rule requires you to look at all of the ways your Customer Information is handled, manipulated, accessed, stored, transmitted, disposed of, etc., and design and implement procedures that will allow you to detect, prevent and respond to attacks, intrusions, or other systems failures that may affect your Customer Information.

What kinds of attacks, intrusions, or other systems failures does the Safeguards Rule cover?

As with the other parts of your risk assessment, you need to focus on detecting, preventing and responding to "reasonably foreseeable" attacks, intrusions, or other systems failures that may affect your Customer Information. It is not at all unlikely that different dealerships will find different threats to be "reasonably foreseeable." This is because any threats your Customer Information may face are largely dependent on how you run your operations. Think about the following in the context of your dealership's operations:

- Is your Customer Information, or the means by which you store Customer Information, vulnerable to fire, flood or other physical damage?
- Are your computer systems equipped with good firewall and anti-virus protection?
- Is your electronic Customer Information password protected and/or encrypted?
- Do you require your employees to keep passwords private?
- Do you limit access to Customer Information to those employees with a "need to know?"
- Do you prohibit employees who are authorized to access Customer Information from granting access to non-authorized personnel?
- Do you routinely lock areas where you access, use or store Customer Information?
- Do you have recovery plans to deal with a loss of your Customer Information?
- Do you have systems in place to identify who accesses your Customer Information?
- Have you trained your employees to recognize attempts by telephone callers to fraudulently obtain information about your customers (pretexting)?
- Do you have procedures for reporting security breaches, misappropriation of Customer Information, fraudulent use of passwords, etc.?
- Do you check back-ups periodically to ensure readability? (or reliability?)

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

What are your responsibilities under the Safeguards Rule with respect to guarding against such attacks, intrusions, or other systems failures?
Your responsibilities under the Safeguards Rule are pretty straightforward. Once you identify "reasonably foreseeable" attacks, intrusions, or other systems failures that may affect your Customer Information, you must determine whether your current policies for detecting, preventing and responding to such compromises adequately address the risk, and if not, design and implement new policies that do.

While large dealer groups may have policies that address compromise of their Customer Information, many small and mid-size dealers may not. It is important that all dealers take this and other requirements imposed by the Safeguards Rule seriously. Consider working with your legal counsel and consultants when drafting the required procedures.

What safeguards should you consider?
As with all of your actions under the Safeguards Rule, you must tailor your safeguards to your operations. The following are some safeguards to consider:

- Keep your paper-based Customer Information stored in fire/flood protected areas.
- Use adequate firewall and updated anti-virus protection.
- Require the use of strong passwords and/or encryption.
- Prohibit the disclosure of passwords.
- Manage and monitor password use and Customer Information access.
- Lock areas where you access, use or store Customer Information, and monitor and audit key distribution.
- Back up your electronic Customer Information frequently, and keep it in a secure and climate-controlled location.
- Discipline personnel who violate your information security policies.

The FTC's suggestions on ways to effectively manage systems failures are set forth at **Appendix I.**

4. Risk Assessment -- Other Areas of Your Operation

To the extent you identify in your risk assessment other areas of your operations where there are potential threats to the safety, security and integrity of your Customer Information, you should follow a process similar to that outlined above. That is, identify the reasonably foreseeable risks to your Customer Information, determine whether your current safeguards are adequate, and if not, design and implement new safeguards that are.

C. Designing and Implementing Information Safeguards to Control Risks Identified in Your Risk Assessment

Once you have completed your risk assessment and have determined that your current safeguards are not sufficient to protect against the reasonably foreseeable risks you have identified, the Safeguards Rule charges you with the task of designing and implementing new safeguards that are.

As you may recall, the Privacy Rule requires you to give a brief description of your safeguards in your privacy notices. The Privacy Rule included some "model" language for your privacy notices, e.g., "*we maintain physical, electronic, and*

procedural safeguards that comply with federal regulations to guard your nonpublic personal information," and indicated that you could use that language to comply with the Privacy Rule, provided it was true and accurate. At that time, knowing that the Safeguards Rule would not be immediately forthcoming, the FTC indicated its expectation that "each [dealer] will have in place at least the administrative or other safeguards necessary to honor any opt-out requests made by consumers under the Privacy Rule."

Your obligations under this element of your Information Security Program go far beyond your ability to honor requests by your customers or consumers to opt-out of certain of your information-sharing practices (to the extent your practices require you to offer an opt-out right in your privacy notice). The Safeguards Rule requires you to determine your risks, evaluate your current safeguards, and then implement additional safeguards where your current ones are deficient. You will need to determine what, if any, additional safeguards you need to implement as a result of your risk assessment, taking into account:

- The size and complexity of your dealership(s) and its operations;
- The nature and scope of your dealership(s)' finance and lease activities; and
- The sensitivity of the Customer Information you collect, store, transmit, etc.

How do you determine whether your current policies and procedures are sufficient?

This is one of the most subjective aspects of your compliance effort. The FTC recognizes that dealers must focus their limited resources on addressing those risks that are most relevant to their individual operations. The Safeguards Rule applies the FTC's "flexible" standard so that you have great flexibility in determining what safeguards are appropriate for you.

In effect, you need to balance the safeguards you implement against the FTC's three pronged "flexible" standard. For example:

- The greater the size and complexity of your dealership(s) and its operations, the more sophisticated your safeguards will be.
- The greater number of finance and lease transactions you originate, the more safeguards you will likely need to put in place.
- The more sensitive the Customer Information you collect, store, transmit, etc., is, the more safeguards you will have in place. Note that for this prong, credit applications and consumer reports likely contain some of the most sensitive Customer Information you possess, so to the extent you do a significant volume of finance and/or lease transactions, you will need to think carefully about what safeguards are appropriate.

How sophisticated must your safeguards be?

The nature and sophistication of your safeguards will depend largely on the nature and sophistication of your operations. It will also depend on available technology and the cost of such technology as compared to the relative benefit it provides in securing your Customer Information. Note the following examples:

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

Example: You own a small dealership and finance or lease most of your vehicles. In your office, you have a computer that you use to transmit some Customer Information, but typically you use a fax machine to transmit Customer Information to finance companies. You do not keep electronic records of Customer Information, but keep deal jackets and other paper files in your office.

- *In the example above, all of the Customer Information activities take place in a single office. You should keep it locked, and only permit authorized persons to have access.*
- *Paper files should be kept in locked cabinets, away from cleaning services, etc., who may have reason to be in your office.*
- *You should install a firewall and anti-virus software on your computer, and use a password-protected screensaver.*
- *You should shred documents containing Customer Information prior to disposal, and/or use a bonded and secure disposal service.*
- *Do not leave Customer Information (e.g., a credit application) in your fax machine.*

How will you know if your new safeguards are compliant?
Because the FTC's "flexible" standard is subjective, it will be hard to know if you "did it right." However, there are some steps you can take to increase your confidence in your compliance efforts:

- Prepare and maintain your Information Security Program with due regard for all five required elements.
- Use your experienced employees to assist you in the design, implementation and maintenance of your Information Security Program.
- Use outside experts in those areas where you do not have expertise among your staff.
- Have your legal counsel and a consultant who is familiar with your operations and with the Safeguards Rule review your Information Security Program.
- Even though it is not required, document your risk assessment activities. It will help you in your audit and monitoring obligations, as well as in the event of an external investigation.

D. Regularly Testing or Auditing the Effectiveness of Your Safeguards' Key Controls, Systems, and Procedures

The Safeguards Rule requires you to:

- Design and implement information safeguards to control the risks you identify through your risk assessment; and
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

What are key controls, systems, and procedures?
Your key controls, systems and procedures are the operational portions of your Information Security Program. These would include, among other things:

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- Your computer data protection systems, e.g., firewalls, virus software, password systems, etc.
- Electronic and non-electronic data storage systems and procedures, e.g., door locks, filing cabinet locks, computer server security systems, disposal systems, etc.
- Customer Information access procedures, e.g., log in/log out procedures, password distribution, key distribution, etc.

In essence, these things are the operational tools that make your Information Security Program work. You need to monitor and test these systems on a periodic basis.

What are some examples of appropriate testing or monitoring?
Appropriate testing and monitoring necessarily turns on the FTC's three-pronged "flexible" standard, that is, the appropriateness of your testing and monitoring will correlate with the size and complexity of your operations and the sensitivity of the Customer Information being protected. Some examples may be:

- Check to see that doors and cabinets where Customer Information is stored are locked as appropriate, and ensure that keys have been issued only to authorized personnel. Ensure that personnel protect the keys with the same safeguards afforded to Customer Information.
- If you require password-protected computer applications, walk around and try to access various computers to ensure the screensavers are being used.
- Require the use of, and monitor, Customer Information access logs.
- Periodically test your employees on your information safeguarding policies and procedures.
- Monitor your computer servers for unauthorized access.
- Walk around the sales floor of your dealership to see if credit applications or other documents containing Customer Information are left unattended and in plain view or if such documents are being disposed of in trash cans accessible to the public.
- Upgrade your anti-virus software as new threats emerge.

How do you know whether your safeguards are effective?
You will want to discover through your testing and monitoring whether or not your safeguards are effective, as opposed to finding out because one of your customers was harmed by an information security failure. Assuming that you thoroughly test the different elements of your Information Security Program requirements on a periodic basis, compromises should make themselves apparent. It also is a good idea to train your employees to be vigilant. They are often on the front lines, and in the best position to recognize security threats and breaches.

How often must testing/monitoring occur?
The Safeguards Rule does not require a specific period in between tests. Your frequency will depend on what it is you are testing or monitoring. For example:

- You will probably want to check locks on a daily basis.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- Your IT administrator will monitor the effectiveness of your computer firewalls and anti-virus software on an ongoing basis.
- You may want to test your employees on an annual basis.
- You may want to randomly check employee compliance with your safeguarding policies and procedures.

Are there certain instances that require special consideration with respect to testing and monitoring your Information Security Program?
Testing and monitoring should cover all aspects of your Information Security Program. However, you will want to pay particular attention to the three areas identified by the FTC, that is:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to attacks, intrusions, or other systems failures.

E. Overseeing Service Providers

The Safeguards Rule requires you to:

- Oversee your service providers by taking reasonable steps to select and retain service providers that are "capable of maintaining appropriate safeguards" for your Customer Information; and
- Require your service providers by contract to "implement and maintain such safeguards."

As you might imagine, there is no easy means of evaluating a service provider's safeguarding capabilities. The steps that are reasonable under the Safeguards Rule will depend upon the circumstances and the relationship between you and your various service providers, and will likely be different for each service provider, or potential service provider. At a minimum, the FTC has indicated that it expects that each dealer will: (1) take reasonable steps to assure itself that its current and potential service providers maintain sufficient procedures to detect and respond to security breaches, and (2) maintain reasonable procedures to discover and respond to widely-known security failures by its current and potential service providers. This latter requirement means that someone in your operation must be charged with keeping apprised of such failures.

Who qualifies as a service provider under the Safeguards Rule?
The Safeguards Rule defines a "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 [dealer]." This definition includes any independent contractors engaged by a dealer who will have access to Customer Information. Customer Information means information about a consumer with whom you have entered into a finance or lease transaction, for example, information contained in a consumer's credit report or credit application, account numbers, bank balances, etc., lists of the names of your finance and lease customers,

and any Customer Information you receive from other financial institutions (e.g., banks, finance companies, other dealerships, etc.). Examples of service providers include:

- Your DMS, CRM and lead providers;
- Third parties that host F&I platforms; or
- Third parties to whom you outsource functions, such as billing and mailing.

While certain vendors may not necessarily fit the definition of "service provider," you should consider protecting the information you pass along to them as well. **In fact, it would be prudent to make all of your customer data, regardless of whether or not it is Customer Information, subject to your Information Security Program**. By doing so, you will dramatically decrease the risk of violating the Safeguards Rule as to actual Customer Information, as well as provide a valuable service to your customers. In addition, it may simply be more cost effective to provide Safeguards Rule protections to all of your customer data rather than to try to categorize data you receive on a daily basis.

Why must you oversee your service providers?
The general rule is, the FTC oversees your compliance under the Safeguards Rule, and you oversee the vendors to which you outsource certain tasks. Simply put, you are in the best position to police your vendors because you choose them, you have the contact with them, and you can fire them. Also, it is a means for the regulators to maximize their resources. By holding you responsible to some degree for the actions of your vendors, it eliminates an entire class of persons that they must oversee directly.

Must you be certain beyond doubt that your service providers' information security safeguards are adequate?
No. However, you must take "reasonable steps" to select and retain service providers that are "capable of maintaining appropriate safeguards" for your Customer Information. This is an ongoing requirement, that is, you must monitor your service providers to ensure they actually maintain such appropriate safeguards.

What qualifies as "reasonable steps" to use when selecting or determining whether to retain service providers?
The FTC has not yet provided direct guidance on this issue. However, here are some suggestions for determining the adequacy and appropriateness of service providers:

- The ability of the service provider to provide services compatible with your needs.
- Check the references of your potential service providers and check with other customers of the service provider to determine their level of satisfaction.
- Discussing your security needs with your service providers and obtaining representations and warranties from them that they will meet those needs.
- Contracting for the response you expect from the service provider in the event of a security threat or breach.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

- Contracting for the service providers' obligation to maintain a sufficient level of security.
- Contracting for reasonable service and support in terms of maintenance hours, response time, resolution time, security, disaster planning, and other service levels.
- Before contracting with a service provider, run a test of information exchanges with "dummy data" to determine if the proposed exchange is secure. For existing service providers, supplement each batch of your Customer Information available to your service provider with dummy entries, such as account numbers or addresses that you control, and monitor use of these entries to detect unauthorized contacts.
- Determine if the FTC or a federal or state enforcement agency is investigating or has investigated the service provider's information security practices.

Must your service providers use the same safeguards as you do?
No. However, your service providers must be "capable of maintaining appropriate safeguards" for your Customer Information. What is appropriate will depend on what service is being provided. You will probably find it necessary to make a case-by-case assessment to determine what safeguards each service provider should have in place, e.g., it is probably impractical to impose a "one-size-fits-all" standard on your providers. Not only that, but you would likely find yourself unable to negotiate such a standard into your vendor contracts.

The obvious question is whether you are required to review your service providers' Information Security Programs. The answer is "no" – there is nothing in the Safeguards Rule that requires you to do this, and there are a number of reasons why an entity might be reluctant to do so, chief among them, their desire to maintain the confidentiality of their internal security plans. Nevertheless, you should inquire as to the nature of your service providers' security capabilities, and specifically contract for the level of security you require from each of them.

A note about factory and service provider relations
There are many instances in which you will need to communicate information to the factory or other major vendors, e.g., your DMS provider. Keep in mind that the Safeguards Rule does not address *whether* you can share information with these parties. It is the Privacy Rule that governs this. The Safeguards Rule addresses *how* you communicate with these parties.

Must you prepare a separate contract for each of your service providers to require them to implement and maintain adequate safeguards?
The Safeguards Rule provides that you must require, by contract, that your service providers implement and maintain appropriate safeguards. While you may use a separate contract with each of your service providers for this sole purpose, the Safeguards Rule does not require you to do so. You will meet the contracting requirement if you ensure there is appropriate language in your primary contract with your service provider(s).

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

What must your service provider safeguards contract or clause require?
How you choose to contract for this requirement will depend on the nature of the services being provided and/or the sensitivity of the Customer Information involved.

The Safeguards Rule's contracting requirement deals with what third parties must do to *protect your Customer Information*. This should not be confused with the Privacy Rule's requirement that deals with *disclosure of non-public personal information*. Recall that under the Privacy Rule, § 313.13(a)(1), you must enter into a contractual agreement with your service providers that prohibits such parties from disclosing or using non-public personal information that you have disclosed to them, "other than to carry out the purposes for which you disclosed the information, including use under an exception in § 313.14 or 313.15 in the ordinary course of business to carry out those purposes." **The contractual agreement that you currently use for complying with the Privacy Rule may not be sufficient for complying with the Safeguards Rule.**

Samples of possible contract clauses for complying with the Safeguards Rule can be found in **Appendix J.** Remember that whether you use a clause or a separate contract, the language you use will be a function of the nature of the services being provided and the sensitivity of the Customer Information involved. You should involve your legal counsel in drafting appropriate language for your specific situation.

How soon must you have contractual agreements with service providers for information safeguards in place?
May 23, 2003: For all service provider relationships entered into on **June 25, 2002 or later**, you have until **May 23, 2003** to revise your service provider contracts to include a contractual provision requiring the service provider to implement and maintain appropriate safeguards.

May 24, 2004: For all service provider agreements entered into **prior to June 25, 2002**, you have until **May 24, 2004** to revise these contracts to include a contractual provision requiring the service provider to implement and maintain appropriate safeguards.

Are you legally liable for information security breaches that occur at your service provider level?
While you are not directly liable for your service providers breaches, you will be liable to the extent you do not take "reasonable steps" to select and retain service providers that are "capable of maintaining appropriate safeguards" for your Customer Information, or if you fail to require service providers by contract to implement and maintain such safeguards.

In addition, you will want to include indemnification provisions in your service provider contracts, protecting you against any harm that arises out of your service providers' failure to maintain appropriate standards. Consult your legal counsel for appropriate language.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

F. Periodic Reevaluation

The Safeguards Rule requires you to evaluate and adjust your Information Security Program in light of:

- The results of your testing and monitoring efforts;
- Any material changes to your operations or business arrangements; or
- Any other circumstances that you know or have reason to know may have a material impact on your Information Security Program.

What kinds of circumstances require you to reevaluate your Information Security Program?

There are numerous reasons why you would need to reevaluate your Information Security Program. For instance:

- Your testing and monitoring efforts may reveal lapses in security, e.g., "dummy" Customer Information planted by you in the Customer Information accessible by your service provider so that you could monitor the effectiveness of the service provider's safeguards may reveal fraud or mishandling. This would require you to reevaluate your relationship with, and the safeguards of, your service provider.
- You install a new computer network. You will need to run a risk assessment on the network and implement any appropriate safeguards.
- You enter into a new outsourcing arrangement that requires you to transmit Customer Information over the Internet for the first time.
- You add product lines from new manufacturers. This will require you to ensure the safety and integrity of your Customer Information in this new relationship.
- You determine that your Customer Information is being accessed by only one password, when employee-specific passwords have been assigned.
- You become aware of the imminent release of a new computer virus that your anti-virus software may not detect.

What would constitute a "material impact" on your Information Security Program?

In general, any security, integrity or safety breach that could result in harm to a customer would constitute a material impact on your Information Security Program. Your Program should be designed to protect against compromise of your Customer Information, and will be deficient to the extent it fails to do so. "Material impacts" may include:

- Installing a new computer network that is Internet accessible without appropriate firewalls and anti-virus software.
- Granting new service providers access to Customer Information without the requisite contractual provisions.
- Failing to keep your information security technology up to date.
- Failure of your vendors providing licensed computer applications to keep their information security technology up to date.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX A

SAMPLE INFORMATION SECURITY PROGRAM

NOTE: This Sample Information Security Program is for informational purposes only. It may not be suitable for your particular dealership or operations. You are obligated to design and implement an Information Security Program that is appropriate to your dealership and its operations. Consult outside consultants as necessary for assistance in developing an appropriate Information Security Program for your dealership. Ensure the program is reviewed by legal counsel familiar with federal law and applicable state and local law. The italicized language provides options that may or may not be suitable for your dealership. You must decide which, if any, of the italicized language should be included in your written Information Security Program.

Program Objectives

The objectives of this Information Security Program ("Program") are as follows:

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

For purposes of the Program, "customer information" means any information about a customer of the Dealership, or information the Dealership receives about the customer of another financial institution, that can be directly or indirectly attributed to the customer. This Program, in and of itself, does not create a contract between the Dealership and any person or entity.

Program Coordinator(s)

This Program and the safeguards it contemplates shall be implemented and maintained by an employee or employees ("Program Coordinator") designated by the Dealership. The Program Coordinator shall design, implement and maintain new safeguards as he or she determines to be necessary from time to time. The Program Coordinator shall report to the Dealership [*president, managing partner, etc.*] [*and those board members who have responsibility for overseeing the Program*]. The Program Coordinator may delegate or outsource the performance of any function under the Information Security Program as he or she deems necessary from time to time.

In the event the Program Coordinator leaves the employment of the Dealership, the Dealership [*president, managing partner, etc.*] shall take over the responsibilities of the Program Coordinator until a new Program Coordinator is designated.

Risk Assessment

The Program Coordinator shall conduct a risk assessment 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.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

The risk assessment shall cover all relevant areas of the Dealership's operations, as determined by the Program Coordinator. At a minimum, the risk assessment shall cover the following:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to attacks, intrusions or other systems failures.

Once the Program Coordinator has identified the reasonably foreseeable risks to the Dealership's customer information, the Program Coordinator will determine whether the Dealership's current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the Program Coordinator shall design new policies and procedures that meet the objectives of the Program. Final policies and procedures that meet the objectives of the Program shall be made part of the Program.

Audit

The Program Coordinator shall regularly test or audit the effectiveness of the Dealership's safeguards' key controls, systems, and procedures, to ensure that all safeguards implemented as a result of the risk assessment are effective to control the risks identified in the risk assessment. The Program Coordinator shall revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the Program.

Overseeing Service Providers

The Program Coordinator shall be responsible for overseeing the Dealership's service providers who handle or have access to customer information. The Program Coordinator shall take reasonable steps to select and retain service providers that are capable of maintaining safeguards to protect the specific customer information handled or accessed by each service provider that are consistent with the level of safeguards employed by the Dealership for such information.

The Program Coordinator shall review and approve each service provider contract prior to its execution by the Dealership to ensure that each contract contains appropriate obligations of the service provider to comply with the Dealership's safeguarding requirements.

Periodic Reevaluation of the Program

The Program Coordinator shall reevaluate and modify the Program from time to time as the Program Coordinator deems appropriate. The Program Coordinator shall base such reevaluation and modification on the following:

- The results of the Program Coordinator's testing and monitoring efforts;
- Any material changes to the Dealership's operations, business or information technology arrangements; or
- Any other circumstances that the Program Coordinator knows, or has reason to know, may have a material impact on the Program.

In order to assist the Program Coordinator in this regard, the Dealership shall keep the Program Coordinator apprised of the nature and extent of all third party relationships and any operational changes or other matters that may impact the security or integrity of the Dealership's customer information.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

Information Security Policies and Procedures — Employee Training and Management
In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following employee management and training safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. *All employees and independent contractors are responsible for complying with the Dealership's Program.*
2. *The Dealership will check references of each potential employee prior to the commencement of the applicant's employment.*
3. *The Dealership will obtain a consumer report and criminal background check of each applicant prior to the commencement of the applicant's employment.*
4. *All offers of employment shall be subject to satisfactory references and consumer/criminal report investigations.*
5. *All new employees, and independent contractors who perform services in the Dealership, that have access to customer information will participate in the Dealership's information security training. Each person shall sign and acknowledge his or her agreement to abide by the Dealership's Program. Training will recur at least once each year, or sooner, as determined by Dealership management and as required by changes to the Program.*
6. *Such training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information, such as:*

    - *Identifying for employees and independent contractors the types of customer information subject to protection under the Information Security Program.*
    - *Locking rooms and file cabinets where paper records are kept.*
    - *Using password-activated computer software, systems, applications or terminals or an automatic log-off function that terminates access after a short period of inactivity.*
    - *Using strong passwords (at least eight characters long and alpha-numeric).*
    - *Changing passwords periodically, and maintaining the security of passwords.*
    - *Sending electronic information over secure channels only.*
    - *Appropriately disposing of paper and electronic records.*
    - *Other training as determined appropriate by management from time to time.*

7. *The Dealership will take appropriate steps to encourage awareness of, and compliance with, the Program.*
8. *All employees and independent contractors will be permitted to access customer information on a "need–to-know" basis as determined by Dealership management.*
9. *Personnel shall not be permitted to access, use or reproduce customer information, whether electronic or non-electronic, for their own use or for any use not authorized by the Dealership.*
10. *All persons who fail to comply with the Dealership's Program shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services in the Dealership. This remedy shall be expressly provided for in Dealer's agreements with such independent contractors.*

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

Information Security Policies and Procedures – Information Systems
In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following information systems safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. *All records containing customer information shall be stored and maintained in a secure area.*
   - *Paper records shall be stored in a room, cabinet, or other container that is locked when unattended. The Program Coordinator shall control access to such areas.*
   - *All storage areas shall be protected against destruction or potential damage from physical hazards, like fire or floods.*
   - *Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Program Coordinator shall control access to such servers.*
   - *Customer information consisting of financial or other similar information (e.g., social security numbers, etc.) shall not be stored on any computer system with a direct Internet connection.*
   - *All customer information shall be backed up on a [insert periodic frequency] basis. Such back up data shall be stored in a secure location as determined by the Program Coordinator.*

2. *All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis.*
   - *Inbound credit card information, credit applications, or other sensitive financial data transmitted to the Dealership directly from consumers shall use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmission shall be automatic. Consumers shall be advised against transmitting sensitive data, like account numbers, via electronic mail.*
   - *The Dealership shall require by contract that inbound transmissions of customer information delivered to the Dealership via other sources be encrypted or otherwise secured.*
   - *All outbound transmissions of customer information shall be secured in a manner acceptable to the Program Coordinator.*
   - *To the extent sensitive data must be transmitted to the Dealership by electronic mail, such transmissions shall be password controlled or otherwise protected from theft or unauthorized access at the discretion of the Program Coordinator.*
   - *The Program Coordinator shall review all vendor applications to ensure an appropriate level of security both within the Dealership and with the Dealership's business partners and vendors.*

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

3. *All paper transmissions of customer information by the Dealership shall be performed on a secure basis.*
   - *Sensitive customer information shall be properly secured at all times.*
   - *Customer information delivered by the Dealership to third parties shall be kept sealed at all times.*
   - *Paper-based customer information shall not be left unattended at any time it is in an unsecure area.*

4. *All customer information shall be disposed of in a secure manner.*
   - *The Program Coordinator shall supervise the disposal of all records containing customer information.*
   - *Paper based customer information shall be shredded and stored in a secure area until a disposal or recycling service picks it up.*
   - *All hard drives, diskettes, magnetic tapes, or any other electronic media containing customer information shall be erased and/or destroyed prior to disposing of computers or other hardware.*
   - *All hardware shall be effectively destroyed.*
   - *All customer information shall be disposed of in a secure manner after any applicable retention period.*

5. *The Program Coordinator shall maintain an inventory of Dealership computers, including any handheld devices or PDAs, on or through which customer information may be stored, accessed or transmitted.*

6. *The Program Coordinator shall develop and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.*

Information Security Policies and Procedures – Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following attack and intrusion safeguards:

[*Insert safeguards appropriate for your Dealership*]

[Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law]:

1. *The Program Coordinator shall ensure the Dealership has adequate procedures to address any breaches of the Dealership's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.*
2. *The Program Coordinator shall utilize and maintain a working knowledge of widely available technology for the protection of customer information.*
3. *The Program Coordinator shall communicate with the Dealership's computer vendors from time to time to ensure that the Dealership has installed the most recent patches that resolve software vulnerabilities.*
4. *The Dealership shall utilize anti-virus software that updates automatically.*

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

5. *The Dealership shall maintain up-to-date firewalls.*
6. *The Program Coordinator shall manage the Dealership's information security tools for employees and pass along updates about any security risks or breaches.*
7. *The Program Coordinator shall establish procedures to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.*
8. *The Program Coordinator shall ensure that access to customer information is granted only to legitimate and valid users.*
9. *The Program Coordinator shall notify customers promptly if their customer information is subject to loss, damage or unauthorized access.*

Information Security Policies and Procedures – [Insert Operational Area]

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following information systems safeguards:

[*Insert safeguards appropriate for your Dealership*]

* * * * * * * * * *

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX B

GLOSSARY OF TERMS

Consumer – An individual who initiates the process of obtaining or has obtained a financial product or service from your dealership to be used primarily for personal, family or household purposes. Thus, if someone applies for credit to buy a vehicle for personal use, he or she is a "consumer", even if credit is not extended to the individual.

Customer – A consumer who executes a credit or lease agreement, purchases an insurance product or otherwise obtains a financial product or service from your dealership.

Customer Information – Any record containing nonpublic personal information about a customer of your dealership or of another financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of your dealership or its affiliates.

DMS – Dealership Management System.

FTC – Federal Trade Commission; the federal regulatory agency charged with enforcing the Safeguards Rule for automobile dealers.

Firewall – A security scheme that prevents unauthorized users from gaining access to a computer network or that monitors transfers of information to and from the network.

Information Security Program – The administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, secure, store, use, transmit or otherwise handle Customer Information. The term also refers to the written document(s) evidencing these safeguards.

IT Administrator – Information Technology Administrator; the person(s) responsible for maintaining and/or troubleshooting a dealer's computer systems and programs.

Nonpublic Personal Information – Personally identifiable financial information provided by a consumer to a dealer or otherwise obtained by the dealer, 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. This includes any information a consumer provides to obtain credit or a lease, or any information about the consumer derived from a credit or lease transaction. It also includes a list consumers or customers of financial products or services or the fact that a person is or has been a consumer or customer of a dealer for a financial product or service. Additionally, information a dealer collects through Internet "cookies" in connection with an inquiry about a financial product or service is considered nonpublic personal information. The term does not include aggregate information or blind data that does not contain personal identifiers, such as account numbers, names, or addresses.

PDA – Personal Digital Assistant (e.g., PalmPilots or other handheld devices).

Privacy Notice – Any initial or annual notice required to be provided to your consumers or customers under the FTC's Privacy Rule, as discussed in NADA's "A Guide to the FTC Financial Privacy Regulation," (2001).

Privacy Rule – 16 CFR Part 313, promulgated by the FTC pursuant to mandate under the Gramm-Leach-Bliley Act (15 USC §§ 6801 *et seq*.).

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

Program Coordinator – Individual(s) responsible for implementing, overseeing, and ensuring compliance with a dealer's Information Security Program.

Risk Assessment – The process of reviewing and analyzing a dealer's information security policies and procedures to determine whether the policies or procedures adequately protect Customer Information.

Safeguards Rule – 16 CFR Part 314, promulgated by the FTC pursuant to mandate under the Gramm–Leach–Bliley Act (15 USC §§ 6801 *et seq*.).

Service Provider – Any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to a dealer.

Strong Password – Passwords that are at least 8 characters long, and are comprised of both alpha and numeric characters.

Third-party software or platform – A program provided by a service provider through which dealers may access Customer Information, such as credit reports.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX C

EXAMPLES OF "REASONABLY FORESEEABLE" THREATS TO CUSTOMER INFORMATION

It is more than likely a "reasonably foreseeable" risk that sensitive Customer Information is in danger of compromise if:

- Your F&I staff routinely leaves copies of customer applications and contracts on their desks in your unlocked F&I office.
- You do not keep the F&I office locked.
- You do not limit access to sensitive Customer Information to those persons who have a "need to know."
- You keep paper copies of sensitive Customer Information in unlocked or otherwise unsecured storage areas.
- You dispose of sensitive Customer Information in an unsecure manner, e.g., you do not shred paper files that contain sensitive customer information.
- Your computer servers are kept in unlocked and easily accessible areas.
- You do not protect your paper files and computer servers against fire, flood and other physical damage.
- Your computer files containing Customer Information may be accessed without a password.
- You do not require your employees to keep passwords secure.
- You do not regularly back up sensitive Customer Information.
- You do not use updated virus protection software.
- You do not use an adequate firewall to protect your computers from unauthorized access from the Internet.
- You do not regularly download software security patches that are provided by your vendors and/or other reputable sources.
- You have no agreement with your employees and independent contractors regarding their obligations to keep Customer Information safe, and to not misuse or misappropriate such information.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX D

SAMPLE CHECKLIST FOR EVALUATING EMPLOYEE MANAGEMENT AND TRAINING

(Consult with legal counsel about an appropriate checklist to use for your dealership)

- ☐ Has information security training been incorporated into your current employee training programs?
- ☐ Do employees, and independent contractors performing services in the Dealership, who will receive or have access to Customer Information as part of their job receive information security training before they receive or have access to this information?
- ☐ Have all current employees been required to sign an acknowledgement prior to May 23, 2003 that they will comply with your Information Security Program? Are all new employees hired on or after May 23, 2003 required to sign an acknowledgement before being given access to Customer Information?
- ☐ Are employees being trained on the impact of your Information Security Program on your relationships with service providers?
- ☐ Are the individuals who will conduct your Information Security Program training for your employees receiving training in this area? Are you incorporating periodic "train the trainer" programs to maintain a "cutting edge" training program? If you outsource this training function, is your service provider incorporating these practices?
- ☐ Is your Program Coordinator involved in industry groups or regularly attending seminars to maintain his or her competency in this area?
- ☐ Are employees being trained on how to respond to "pretext calls" (e.g., calls from individuals attempting to obtain information about your customers)?
- ☐ Do employees receive a copy of your written Information Security Program or do they have access to a copy maintained in your dealership?
- ☐ Do employees have unrestricted access to your Program Coordinator so that they may ask questions or report concerns about information security?
- ☐ Are employees receiving periodic training on your Information Security Program and the requirements of the FTC's Safeguards Rule?
- ☐ Are changes to your Information Security Program being communicated to employees in a timely manner?
- ☐ Is senior management and/or your Board of Directors also receiving training on your Information Security Program and the requirements of the FTC's Safeguards Rule?
- ☐ If you provide copies of your written Information Security Program to your employees, are they required to return these copies upon termination of their employment?
- ☐ Does the design of your physical facilities permit unauthorized persons to have access to Customer Information (e.g., Are computer terminals on which credit application information is displayed visible by customers through your display room windows? Can telephone conversations with finance companies be overheard by other customers in your dealership?)?
- ☐ Do you have programs in place to periodically monitor an employee's compliance with your Information Security Program?
- ☐ Are there procedures in place to discipline an employee if the employee violates your Information Security Program?
- ☐ Has your dealership incorporated sufficient background screening for prospective new hires to identify whether individuals have been convicted of the crime of identity theft or similar acts?

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX E

SUGGESTED SAFEGUARDS FOR EMPLOYEE MANAGEMENT AND TRAINING

The following is based on FTC suggested safeguards for employee management and training: [24]

- To the extent permitted by state law, check references and criminal backgrounds prior to hiring employees who will have access to Customer Information.
- Ask every new employee to sign an agreement to follow your dealership's confidentiality and security standards for handling Customer Information. **See Appendix F** for sample language.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of Customer Information, such as:
    - Locking rooms and file cabinets where paper records are kept;
    - Using password protection to access computer terminals or programs at which Customer Information (e.g., credit applications, credit reports) is accessed or is accessible and using time-out procedures for such terminals or programs;
    - Using strong passwords (e.g., at least eight characters long and alpha-numeric);
    - Changing passwords periodically, and not posting passwords near employees' computers;
    - Adopting security procedures (e.g., encryption) for sensitive Customer Information when it is transmitted electronically over networks or stored online;
    - Referring calls or other requests for Customer Information to designated individuals who have had safeguards training; and
    - Recognizing any fraudulent attempt to obtain Customer Information and reporting it to appropriate law enforcement agencies.

- Instruct and regularly remind all employees of your dealership's policy — and the legal requirement — to keep Customer Information secure and confidential. You may want to provide employees with a detailed description of the kind of Customer Information you handle (name, address, account number, and any other relevant information) and post reminders about their responsibility for security in areas where such information is stored — in file rooms, for example.
- Limit access to Customer Information to employees who have a business reason for seeing it. For example, grant access to Customer Information files to employees who respond to customer inquiries, but only to the extent they need this information to do their job.
- Impose disciplinary measures for any breaches.

APPENDIX F

SAMPLE LANGUAGE FOR EMPLOYEE ACKNOWLEDGEMENT OF INFORMATION SAFEGUARDING OBLIGATIONS

(Consult with legal counsel about appropriate language to use for your dealership)

Employee Acknowledgement of and Agreement to Comply with Information Security Program

I, _____, acknowledge that I have read and agree to comply with the policies and procedures regarding the safeguarding of customer information, as outlined in [*Dealer's*] Information Security Program. I agree to comply with Dealer's information safeguarding policies and procedures, and any amendments or additions to these policies and procedures that Dealer may make from time to time.

I will not intentionally share or disclose, or cause to be shared or disclosed, any customer information to any person or entity in violation of Dealer's information security policies and procedures. Further, I will not intentionally view or access, or caused to be viewed or accessed, any customer information in violation of Dealer's information security policies and procedures. I will at all times strive to protect and secure all customer information that I may receive or have access to during the course of my employment in compliance with Dealer's information security policies and procedures. I will not remove from the Dealer's place of business any Customer Information or written or electronic materials documenting the Dealer's Information Security Program. I understand that in the event I fail to abide by Dealer's information safeguarding policies and procedures, whether my failure is intentional or unintentional, I will be subject to disciplinary action. This disciplinary action may include termination of my employment with Dealer or any other disciplinary measures as provided in [*Dealer's Employee Handbook*][*Dealer's Information Security Program*].

_____ _____

Employee's Signature Date

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX G

GOOD V. RISKY PRACTICES

Assessing the Adequacy of Your Customer Information Systems Safeguards

Because each dealer's operations will be different, it is impractical to give you a list of safeguards "guaranteed" to meet FTC standards. However, the following list is offered as general guidance with the understanding that some of the "good" practices listed below may not be suitable for your operations. You must tailor your safeguarding practices to meet the objectives of the Safeguards Rule in the context of your operations.

Good Practices	*Risky Practices*
F&I Office kept locked with access only to F&I personnel and management.	No controls or limitations on employee/other access.
Customer Information password protected with multiple layers of security.	Records stored in unlocked rooms/containers.
Use of strong firewalls and anti-virus software.	Passwords not required; Multiple persons using the same password.
Employee access to Customer Information on a "need to know" basis, with accountability, e.g., log in and log out dealer jackets, etc.	Employees permitted access to sensitive Customer Information without accountability.
Safeguards training for all applicable personnel.	No use of adequate firewalls or updated anti-virus software.
Secure Internet transmissions.	No formal safeguards training program.
Sealed courier packs, with safeguards training for internal couriers.	Paper records left in unsecured locations.
Use of strong encryption software.	Unencrypted sensitive emails.
Computer terminals and applications with password access and time-out functions.	Unsealed courier packs.
Oversight of third party processors to ensure use of appropriate safeguards.	Use of third party processors without appropriate safeguards.
Restrict Customer Information use/access by employees to secure locations.	Customer Information available in unsecured locations; No limits on access to F&I office.
Closing e-mail accounts and changing passwords or access codes when an employee leaves the dealer's employment.	Paper records and computer servers stored in unlocked/unprotected locations.
Use of records retention policy.	No backup or archiving of electronic records/ databases.
Shred paper copies of Customer Information prior to disposal.	No policies/procedures relating to employee interaction with Customer Information.
Use secure waste bins.	No records retention policy.
Use reputable document storage and disposal vendors.	Unsecure disposal/storage practices, e.g., storing backups in cars, garages or basements.
Ensure software and/or systems through which Customer Information may be accessible have adequate safeguards.	

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX H

SUGGESTED SAFEGUARDS FOR CUSTOMER INFORMATION SYSTEMS

The following suggestions on how to safeguard your information systems throughout the life cycle of Customer Information — that is, from collection to disposal, are based on safeguarding suggestions by the FTC:[25]

1. Store records containing Customer Information in a secure area. Make sure only authorized employees have access to the area. For example:
    - Store paper records in a room, cabinet, or other container that is locked when unattended;
    - Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
    - Store electronic Customer Information on a secure server that is accessible only with a password — or has other security protections — and is kept in a physically-secure area;
    - Don't store sensitive Customer Information on a machine with an Internet connection; and
    - Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically secure area.

2. Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit Customer Information electronically:
    - If you collect credit card information, credit applications, or other sensitive financial data, use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the information is encrypted in transit;
    - If you collect information directly from consumers, make secure transmission automatic; Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
    - If you must transmit sensitive data by electronic mail, ensure that such messages are protected, such as by use of passwords, so that only authorized employees have access.

3. Dispose of Customer Information in a secure manner. For example:
    - Ensure that the procedure for disposing records containing Customer Information is approved by the Program Coordinator;
    - Shred or recycle Customer Information recorded on paper and store it in a secure area until a recycling service picks it up;
    - Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain Customer Information;
    - Effectively destroy the hardware; and
    - Promptly dispose of outdated Customer Information after any applicable required retention period.

4. Use appropriate oversight or audit procedures to detect the improper disclosure or theft of Customer Information. For example, supplement each of your customer lists with at least one entry (such as an account number or address) that you control, and monitor use of this entry to detect all unauthorized contacts or charges.

5. Maintain a close inventory of your computers, including any handheld devices or PDAs, on or through which Customer Information may be stored, accessed or transmitted.

APPENDIX I

SUGGESTED SAFEGUARDS FOR MANAGING SYSTEMS FAILURES

The FTC suggests you consider the following ways to maintain up-to-date and appropriate programs and controls, as applicable to your dealership[26]:

- Follow a written contingency plan to address any breaches of your physical, administrative or technical safeguards;
- Check with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
- Use anti-virus software that updates automatically;
- Maintain up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other off-site locations;
- Provide central management of security tools for your employees and pass along updates about any security risks or breaches;
- Take steps to preserve the security, confidentiality and integrity of Customer Information in the event of a computer or other technological failure. For example, back up all customer data regularly;
- Maintain systems and procedures to ensure that access to Customer Information is granted only to legitimate and valid users. For example, use tools like passwords combined with personal identifiers to authenticate the identity of customers and others seeking to do business with your dealership electronically; and
- Notify customers promptly if their Customer Information is subject to loss, damage or unauthorized access (some state laws may also require this).

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

APPENDIX J

SAMPLE INFORMATION SAFEGUARDING CLAUSES TO USE IN SERVICE PROVIDER CONTRACTS

(Consult with legal counsel about appropriate language to use for your dealership)

1. Service Provider agrees to implement and maintain physical, electronic, and procedural safeguards as may be required by Dealer from time to time in Dealer's sole discretion to guard all information and data relating to Dealer's customers to which Service Provider has access pursuant to the terms of this Agreement. Such safeguards shall, at a minimum, comply with applicable federal, state and local laws and regulations.

or

2. Service Provider represents and warrants to Dealer that Service Provider presently maintains, and will continue to maintain and periodically test the efficacy of, appropriate information security programs and measures designed to ensure the security and confidentiality of "Customer Information" (as defined in 16 CFR § 314.2(b)). Such information security programs and measures shall include appropriate procedures designed to (1) protect the security and confidentiality of such information, (2) protect against anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer of Dealer. Dealer, its representatives and applicable governmental regulators may, from time to time, also audit the security programs and measures implemented by Service Provider pursuant to this Section, and Service Provider shall not impose any fees or charges on Dealer, its representatives or applicable governmental regulators in connection with any such audit.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

END NOTES

[1] 15 U.S.C. § 6801(a)(2002); 16 C.F.R. Part 313(2002).
[2] 16 C.F.R. Part 314.
[3] 15 U.S.C. §§ 6802(a), 6803(2002).
[4] 15 U.S.C. § 6801(b)(2002).
[5] 15 U.S.C. § 6801(b)(2002).
[6] 16 C.F.R. § 313.6(a)(8)(2002).
[7] See 16 C.F.R. Part 313(2002), Appendix A, Sample Clause A-7.
[8] 16 C.F.R. § 313.3 (k)(1)(2002).
[9] 15 U.S.C. § 6809(3)(A)(2002); 12 U.S.C. § 1843(k)(4)(6)(2001); 12 C.F.R. § 211.10(a)(2)&(3)(2002).
[10] 15 U.S.C. § 6805(a)(6)(2002).
[11] 15 U.S.C. § 6809(9)(2002).
[12] 16 C.F.R. § 314.2(a); 16 C.F.R. § 313.1(b)(2002).
[13] 16 C.F.R. §§ 314.1(a), 314.3.
[14] 16 C.F.R. § 314.2(b).
[15] 16 C.F.R. §§ 314.2(b), 314.1(b).
[16] 16 C.F.R. §§ 314.2(b); 16 C.F.R. § 313.3(n)(1)(ii)(2002).
[17] 16 C.F.R. §§ 313.3(e), 313.3(h)(2002).
[18] 16 C.F.R. § 314.4(d)(1).
[19] 67 Fed. Reg. 36,484(May 23, 2002).
[20] See 16 C.F.R. §§ 313.13, 313.14 and 313.15(2002).
[21] See 16 C.F.R. § 313.10(2002).
[22] 15 U.S.C. § 6805(a)(7)(2002).
[23] See "Interagency Guidelines Establishing Standards For Safeguarding Customer Information," at III(A)&(F), 66 Fed. Reg. 8,616-8,641(February 1, 2001).
[24] See FTC publication, "Financial Institutions and Consumer Data: Complying with the Safeguards Rule," at http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.
[25] Id.
[26] Id.

Published by the National Automobile Dealers Association
8400 Westpark Drive, McLean, VA 22102

ACKNOWLEDGMENT

This management guide was prepared for NADA by

Michael A. Benoit, Esq.
Hudson Cook, LLP
971 Corporate Blvd.
Suite 301
Linthicum, MD 21090-2232

NADA-ATD
Resource Toolbox

National Automobile Dealers Association
8400 Westpark Drive
McLean, Virginia 22102-3591

http://www.NADAuniversity.com

ATD
AMERICAN TRUCK DEALERS
A DIVISION OF NADA