

## **FTC regulations require dealers to protect customer information**

The regulation requires all dealers "to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

### **What does the FTC consider "Customer Information"?**

In simple terms, the regulations want you to protect nonpublic personal information (NPI). For dealers, this can be defined as any personally identifiable financial information that a dealer collects about an individual in connection with providing a finance contract, lease or insurance-unless that information is otherwise publicly available. Some examples of nonpublic customer information identified by the FTC include:

- Any information an individual provides you to get a financial product including name, address, income, Social Security number or other information on an application.
- Any information you obtain about a customer during the financing process including bank or loan account numbers, credit cards, loan or deposit balances, payment history and credit history reports.
- Any lists of customers derived even partially from NPI. For example, a dealer's list of finance and lease customers that identifies a customer by name would be considered NPI.

### **5 Elements Required for Compliance**

The regulations require that dealers develop a written plan and include the following five elements in their security programs:

1. Designate an employee to coordinate your information security program.
2. Identify reasonably foreseeable risks to your customer information that could result in unauthorized disclosure, misuse, alteration or destruction. Assess the sufficiency of any safeguards in place to control these risks.
3. Design and implement safeguards to control the risks identified above. Regularly test or otherwise monitor the effectiveness of your program.
4. Oversee your service providers by taking reasonable steps to select and retain providers that are capable of maintaining the appropriate security of your customer information. You should require your service providers-by contract-to implement and maintain security measures.
5. Evaluate and adjust your security program based on the results of testing performed in accordance with step 3 above and any material changes to your business operations.

In developing your security program, the regulations require you to consider each relevant area of your operations. These include employee training and management; information systems, including the way you process, store, transmit and dispose of information, both written and electronic; and detecting, preventing and responding to attacks, intrusions or other security program failures.

As you can see from the five elements, the regulations not only require you to undertake actions to get into compliance, but you are also required to take prescribed actions, such as testing your security program, to stay in compliance. If you are not in compliance, the FTC can levy a fine of up to \$11,000 per day.

### **Tips for Developing Your Program**

Make sure you address all of the required elements of the regulations. Simply typing up a policy is not enough. A policy does not equate to a "program" in the eyes of the FTC.

1. Identify the person who will be "in-charge" of your program. The term commonly being used is "Program Coordinator". Be sure you give this person the time it will take to develop an appropriate program and the proper amount of authority to get you in compliance and keep you there.
2. Prepare a written risk assessment. Nowhere in the regulations does it say that you are required to have anything other than your policies in writing, but practically speaking there are three good reasons to do so:
  - You will be able to organize your policies so that they address all of the risks identified.
  - If the FTC comes knocking, you will be able to easily demonstrate that you complied.
  - All of the attorneys who have spoken at seminars on this topic say repeatedly to document, document, document!
3. Make a list of your risks and threats identified during your assessment.
4. Prepare written policies that not only address the specific requirements you intend for each employee to follow; but also management's plans to deal with all elements of your program. Examples of areas you should consider including in your policies are:
  - Program Coordinator duties
  - Handling and reporting breeches or violations of your security program
  - Employee training and orientation procedures
  - Hiring and screening process
  - Program testing plans
  - Computer access and security rules
5. Train your employees. First, employees must be trained so that they are aware of, and understand, the FTC Safeguards Rule. Secondly, you must train your employees so that they are informed of your dealership's specific policies in your security program. Be sure to keep a log of all employees who attend training.
6. Have all employees sign an agreement to follow your company's security polices as well as acknowledge that they have been properly trained.
7. Create testing procedures that can be conducted on a regular basis. Create a log or some other way to track your testing history. Again, if the FTC comes, you want to be ready. No matter how you choose to attack the development of your Information Security Program, a significant amount of time and effort will be required by your organization. Dealers should focus on developing a comprehensive program that addresses all of the required elements.