ZURICH®

Loss Prevention

Please route to:

- Owner
- General manager
- Sales manager
- Service manager
- Office manager

Protecting your customers' information: The Safeguards Rule

The Federal Trade Commission (FTC) enacted Standards for Safeguarding Customer Information ("Safeguards Rule") on May 23, 2003. By now, most dealerships should have implemented their information security programs and taken steps to ensure compliance with the Safeguards Rule. If you have not, we recommend taking steps to get in compliance immediately. If you have, it's still important to periodically review and assess your program to ensure you remain in compliance.

History

President Clinton signed the Gramm-Leach-Bliley Act ("GLB Act") into law on November 12, 1999. In addition to reforming the financial services industry, the GLB Act included provisions for how "financial institutions" should share and protect their customers' non-public personal information.

As a result of its passage, the GLB Act required the FTC and other government agencies that regulate financial institutions to implement regulations to carry out the GLB Act's provisions. The regulations required all covered businesses to be in full compliance by July 1, 2001.

The FTC first issued the Privacy of Consumer Financial Information Rule ("Privacy Rule") to address provisions in the GLB Act about how customer information is shared. The Privacy Rule defines "consumers" and "customers" and deals with how you share information about customers who obtain or apply for credit or lease products from you.

Following the Privacy Rule, the FTC then enacted the Safeguards Rule to address provisions in the GLB Act regarding how customer information is protected. The Safeguards Rule deals with how you protect information about your finance and lease customers.[1, 2, 3, 4]

Who must comply with the Safeguards Rule

The definition of "financial institution" includes many businesses that may not normally describe themselves that way. In fact, the Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. While the FTC has never defined the phrase "significantly engaged," you should consider yourself "significantly engaged" in financial activities for purposes of the Safeguard Rule if you regularly provide installment sale and/or lease financing to consumers, even if you immediately assign sales and lease contracts to bank or finance company.[2, 3]

Objectives of the Safeguards Rule

In order to understand the objectives of the Safeguards Rule, it's important to recognize why the GLB Act required the FTC and other government agencies to enact rules to protect sensitive customer information.

Identify theft and customer data breaches are now common place, with stories found frequently in the news. In one case several years ago, an employee of a software vendor, who provided services to the three national credit agencies, sold customer information to identity thieves. At last report authorities knew of at least 30,000 victims and an estimated $2.7 million in losses.

Consider the amount of current and historical customer data your business has accumulated over the years. It could be stored in paper format in a file drawer, or digital format on a computer hard drive. Now consider how safe and secure that information is. The objective of the Safeguards Rule is to:

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

Assess your compliance

The Safeguards Rule requires companies to develop and implement an information security program. As part of the program, each company must[2]:

- Have a written information security plan that describes the actions and steps your business will take to protect customer information. The Safeguards Rules specifies the size of your plan should be appropriate to your dealerships' size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue
- Designate one or more employees to coordinate your security plan. These employee(s) should be documented in your written security plan, and aware that they have been so designated. In addition, it is recommended you update the written plan coordinators names in the security plan as personnel changes.
- Identify and assess the risks to customer information in each relevant area of your organization's operation. In addition, you should evaluate the effectiveness of current safeguards for controlling these risks at reasonable intervals.
- Routinely monitor and test their information security program.
- Select appropriate service providers and require them, by contract, to implement safeguards that are appropriate to their organization in protecting consumer information.
- Evaluate all aspects of your program from time to time, to make appropriate adjustments and to explain why you believed the adjustments were appropriate.

Securing your information

The Safeguards Rule requires that you consider risks to customer information in all areas of your operation, with special emphasis on three critical areas: Employee Training and Management; Information Systems; and Detecting and Managing System Failures. Please refer to the full Safeguards Rule, referenced at the end of this bulletin, for the complete content and practices to be implemented.[1]

Employee training and management

The success or failure of your information security program depends largely on the employees who implement it. Some best practices to consider[2]:

- Check references prior to hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your organization's confidentiality and security standards for handling customer information.
- 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 strong passwords, at least eight characters long.
  - Encrypting 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.
- Regularly instruct and remind all employees of your organization'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.
- 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 it to do their job.

Information systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Below are some suggestions on how to maintain security throughout the life cycle of customer information—that is, from data entry to data disposal[2]:

- Store records 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.
  - 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 data on a machine with an Internet connection.
  - Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically secure area.
- Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information. Specifically:
  - If you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail.
  - If you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.
- Dispose of customer information in a secure manner and, where applicable, consistent with the FTC's Disposal Rule, www.ftc.gov/os/2004/11/041118disposalfrn.pdf. For example:
  - Hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information.
  - Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up, and promptly dispose of outdated customer information.
- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.

Managing system failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures. Consider the following suggestions[2]:

- Maintain up-to-date and appropriate programs and controls by:
  - Following a written contingency plan to address any breaches of your physical, administrative or technical safeguards.
  - Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities.
  - Using anti-virus software that updates automatically.
  - Maintaining 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.
  - Providing central management of security tools for your employees and passing 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 nonpublic consumer information is granted only to legitimate and valid users.
- Notify customers promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

Additional Resources

Safeguards Rule

- Safeguards Rule: www.ftc.gov/os/2002/05/67fr36585.pdf
- How to Comply With the Safeguards Rule: business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule
- NADA "A Dealer Guide to Safeguarding Customer Information": www.nada.org/NR/rdonlyres/3034050F-0D43-4E69-9AD3-85C39959F89E/0/SafeguardingCustomerInfo.pdf

Privacy Rule

- Privacy Rule: www.ftc.gov/os/2000/05/65fr33645.pdf
- How to Comply With the Privacy Rule: business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act
- Privacy Rule FAQs for Auto Dealers: business.ftc.gov/documents/bus64-ftcs-privacy-rule-and-auto-dealers-faqs

Gramm-Leach-Bliley Act

- GBL Act: www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
- Bureau of Consumer Protection - GBL Act: business.ftc.gov/privacy-and-security/gramm-leach-bliley-act

References

[1] www.ftc.gov/os/2002/05/67fr36585.pdf

[2] business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule

[3] www.nada.org/NR/rdonlyres/3034050F-0D43-4E69-9AD3-85C39959F89E/0/SafeguardingCustomerInfo.pdf

[4] business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

Loss prevention information

For questions about this loss prevention topic, contact the Zurich Risk Engineering Department at 800-821-7803.

Not a customer?

For more information about Zurich's products and Risk Engineering services, visit www.zurichna.com/zdu or call us at 800-842-8842 ext. 7449.

Already a customer?

Contact your Zurich Account Executive or agent for information about additional Zurich's products and Risk Engineering services.