

# An Overview of the **Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule**



## **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

# An Overview of the **Gramm-Leach-Bliley (GLB) Act** and the **Safeguards Rule**

## FTC FACTS for Business

ftc.gov  
Federal Trade Commission  
1-877-FTC-HELP

### Financial Institutions and Customer Information:

## Complying with the Safeguards Rule

**M**any companies collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. **1** The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as “financial institutions” to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. **2** Regarding customer information isn’t just the law. It also makes good business sense. **2** When you show customers you care about the security of their personal information, you increase their confidence in your company. The Rule is available at [www.ftc.gov/privacy/privacyinitiatives/safeguards\\_1&r.html](http://www.ftc.gov/privacy/privacyinitiatives/safeguards_1&r.html).

### WHO MUST COMPLY?

**3** The definition of “financial institution” includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are “significantly engaged” in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit reporting agencies and ATM operators that receive information about their customers. **4** Financial institutions. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

For more information on whether the Safeguards Rule applies to your company, consult section 313.3(k) of the GLB Privacy Rule and the Financial Activities Regulations. Both are available at [www.ftc.gov/privacy/privacyinitiatives/financial\\_rule\\_1&r.html](http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_1&r.html).

### HOW TO COMPLY

**5** The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be

## An Overview of the **Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule**

Assisting dealers with compliance of federal and state regulations impacting data security are key factors that drive many ERA<sup>®</sup> system enhancements. Understanding the complexities of the regulations and responding appropriately is a job that Reynolds takes very seriously. The GLB Act and Safeguards Rule are important drivers of Reynolds' Data Management strategy. This overview is intended to provide you with information directly from the Federal Trade Commission (FTC) regarding complying with the Safeguards Rule. We have provided comments and examples to reinforce how Reynolds responds to this legislation.

- 1 GLB requires companies covered by the rule to ensure the security and confidentiality of sensitive information.
- 2 You should consider the cost of a loss of reputation in your market in addition to the potential fines, penalties, and legal costs associated with a data breach.
- 3 Dealerships have been defined as “financial institutions” relative to GLB.
- 4 This reinforces the importance of dealers selecting reputable partners with a focus on prudent data management and security and to closely monitor their data movement in and out of their DMS.
- 5 It's important to note that some state legislation requires a written plan as well.

### **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

# An Overview of the Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule

## Facts for Business

appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- ✓ designate one or more employees to coordinate its information security program;
- ✓ identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- ✓ design and implement a safeguards program, and regularly monitor and test it;

**1** select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and

- ✓ evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. Companies should implement safeguards appropriate to their own circumstances. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents — say, one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may assign this responsibility to several employees who will work together. In addition, companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network.

## SECURING INFORMATION

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: *Employee Management and Training*; *Information Systems*; and *Detecting and Managing System Failures*. One of the early steps companies should take is to determine what information they are collecting and storing, and whether they have a business need to do so. You can reduce the risks to customer information if you know what you have and keep only what you need.

Depending on the nature of their business operations, firms should consider implementing the following practices:

*Employee Management and Training.* The success of your information security plan depends largely on the employees who implement it. Consider:

- ✓ Checking references or doing background checks before hiring employees who will have access to customer information.
- ✓ Asking every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.

**2** Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.

**3** Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.)

## An Overview of the **Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule**

- 1 The Reynolds Certified Interface (RCI) Program works with third party providers to provide safe, secure, and reliable interfaces to the ERA system.
- 2 ERA setups have always allowed for user access to be controlled based upon the various roles in the dealership.
- 3 ERA requires regular password changes. Passwords must be at least 8 characters and include both alpha and numeric characters.

### **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

# An Overview of the Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule

## 1 Using password-activated screen savers to lock employee computers after a period of inactivity.

- ✓ Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.

- ✓ Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:

- Locking rooms and file cabinets where records are kept;

## 2 Not sharing or openly posting employee passwords in work areas;

## 3 Encrypting sensitive customer information when it is transmitted electronically via public networks;

- Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
- Reporting suspicious attempts to obtain customer information to designated personnel.

- ✓ Regularly reminding all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.

- ✓ Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal

computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.

- ✓ Imposing disciplinary measures for security policy violations.

## 4 Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

*Information Systems.* Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:

- ✓ Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
  - Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
  - Store records in a room or cabinet that is locked when unattended.
  - When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area.
  - Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
  - Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
  - Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.

## An Overview of the **Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule**

- 1 A recent Contact Management enhancement logs users off after 2 hours of inactivity. This is important to ensuring the protection of the sensitive information accessible in Contact Management.
- 2 ERA prohibits a User ID from being logged on to more than one PC at a time.
- 3 An important reason for moving from ERALink to ERAccess was the requirement – for both GLB and many states' legislation – that sensitive ERA data be encrypted, whether the information is passed over the Internet or is contained within the dealership LAN.
- 4 In addition to terminated employees, dealers should also remember to deactivate any User IDs given to terminated vendor partners for the purpose of accessing ERA.

### **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

# An Overview of the Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule

## Facts for Business

✓ Take steps to ensure the secure transmission of customer information. For example:

- When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
- If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.

**1** If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.

✓ Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule, [www.ftc.gov/os/2004/11/041118disposalfrn.pdf](http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf). For example:

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

**Detecting and Managing System Failures.** Effective security management requires your company to deter, detect, and defend against

security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:

- ✓ Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.
- ✓ Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

**2** check with software vendors regularly to get and install patches that resolve software vulnerabilities;

- use anti-virus and anti-spyware software that updates automatically;
- maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
- regularly ensure that ports not used for your business are closed; and
- promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

✓ Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:

**3** keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;

- use an up-to-date intrusion detection system to alert you of attacks;

**4** monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and

## An Overview of the **Gramm-Leach-Bliley (GLB) Act and the Safeguards Rule**

- 1** ERA addressed this important requirement with the Secure Data Connection (SDC) server in 1999. With the move to ERAccess, we are moving to more recent technology to address the need for encrypted movement of data whether it be over the Internet or within the dealership LAN.
- 2** Software Manager for ERA is a great way to ensure ERA systems and users are kept up to date with the most recent software releases and security enhancements.
- 3** Dealerships must take responsibility for monitoring activity and should know who is coming into their system and why – at all times! ERA executable 6240 is an effective tool to monitor this activity.
- 4** Large amounts of transmitted data extracted by third party vendors have been proven to use up to 73% of a dealership's CPU capacity, significantly impacting the performance of the ERA system.

### **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

# An Overview of the **Gramm-Leach-Bliley (GLB) Act** and the **Safeguards Rule**

## Facts for Business

1

**insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.**

- ✓ Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
  - take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
  - preserve and review files or programs that may reveal how the breach occurred; and
  - if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
- ✓ Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
  - notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
  - notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
  - notify the credit bureaus and other businesses that may be affected by the breach. See *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* at [www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm](http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm); and
  - check to see if breach notification is required under applicable state law.

### FOR MORE INFORMATION

Additional guidance is available at [www.ftc.gov/privacy/privacyinitiatives/glbact.html](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html). Resources at that site may alert you to new risks to information security and give people whose information may have been compromised important first-things-first advice for responding. Visit [www.onguardonline.gov](http://www.onguardonline.gov) for information that can help you train your employees in safe computing practices on the job and at home. In addition, the following organizations have information to help you implement appropriate safeguards for your customer data:

Computer Security Resource Center

National Institute for Standards and Technology (NIST)

<http://csrc.nist.gov>

National Strategy to Secure Cyberspace, Department of Homeland Security

[http://www.dhs.gov/files/publications/publication\\_0016.shtm](http://www.dhs.gov/files/publications/publication_0016.shtm)

The SysAdmin, Audit, Network, Security (SANS) Institute

The Top Cyber Security Risks

<http://www.sans.org/top-cyber-security-risks/>

United States Computer Emergency Readiness Team (US CERT)

<http://www.us-cert.gov/resources.html>

Carnegie Mellon Software Engineering Institute CERT Coordination Center

<http://www.cert.org>

## An Overview of the **Gramm-Leach-Bliley (GLB) Act** and the **Safeguards Rule**

- 1 A Reynolds Customer Advisory Board member did this very thing and the results were disheartening – within mere months he began to receive direct mail campaigns addressed to the dummy customer!

In conclusion, the safeguards you implement must be appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of customer information for which you are responsible. There is no one-size-fits-all program for meeting the standards and objectives of the Safeguards Rule. However, compliance with this and other regulations that impact your dealership are critical to your customer relationships and your bottom line. As your trusted partner, you can be confident that Reynolds is constantly working to help you comply with GLB and other federal and state legislation impacting the movement and storage of your dealership data.

Visit **[www.reyrey.com/regulations](http://www.reyrey.com/regulations)** to learn more about state and federal legislation regarding data breach notification laws.

### **Legal Disclaimer:**

This overview is not intended as legal advice and should not be taken as such. We recommend that you consult legal counsel about your dealership's specific compliance obligations under the GLB Act and other laws.

**We appreciate your business and  
we look forward to helping you maximize  
the benefits of your ERA system.**

If you have any questions,  
please call the Technical Assistance Center at  
**800.767.0080.**

Want to get the latest news about  
ERA data management, system updates,  
or the Certified Interface program?  
You can register today and stay informed.

**[www.reyrey.com/email](http://www.reyrey.com/email)**



**Reynolds  
& Reynolds®**

MAKING **BUSINESS** BETTER.