

## Why privacy matters to automotive dealerships

For automotive dealerships, protecting customers' privacy promotes a trust relationship. In the last few years, privacy legislation has given dealerships new incentives to protect customers' non-public personal information—dealerships must implement privacy compliance measures or risk significant penalties.

The new compliance obligations come from lawmakers' efforts to quell a rising tide of harms and burdensome annoyances, including identity theft, irresponsible marketing of account information, telemarketing intrusions, and an explosion of offensive and unsolicited commercial e-mail. Of the recent privacy laws, the Gramm-Leach-Bliley or "GLB" Act<sup>1</sup> of 1999 has posed a unique challenge for automotive dealerships—how to know what protections to implement.

## Why the GLB Act applies to automotive dealerships

The GLB Act, passed by the U.S. Congress in 1999, included new financial privacy requirements for businesses that traditionally hadn't been considered financial institutions—such as automotive dealerships. It is the financing aspect of vehicle transactions that made dealerships accountable for GLB Act compliance.

The GLB Act itself didn't create the regulations businesses must follow. Instead, Congress delegated rulemaking and enforcement authority to several regulatory agencies, each with jurisdiction over different types of businesses. The agency with jurisdiction over automotive dealerships is the Federal Trade Commission (FTC). For dealerships, complying with the GLB Act generally means complying with two rules the FTC created for GLB compliance—the *Privacy Rule* and *Safeguards Rule*.

## The FTC's Privacy Rule

Many people are now accustomed to receiving privacy notices from their banks, credit unions, insurance agencies, and other businesses subject to the GLB Act. According to the FTC, "the [GLB] Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. In turn, consumers have the right to limit some—but not all—sharing of their information." Effective July 1, 2001, the FTC's Privacy Rule<sup>2</sup> affects how automotive dealerships determine who gets to see certain information from or about customers and for what purpose. A dealership must provide customers with privacy notices and—if the dealership engages in certain information-sharing practices—the ability to opt out.

Additional guidance on complying with the Privacy Rule may be on the way. On December 23, 2003, federal regulators invited public comment on proposed new standards for the format and content of privacy notices. In the meantime, dealerships must continue to provide privacy notices prescribed by the current Privacy Rule and share data with manufacturers, service providers, and other third parties only as "permitted by law"—or give customers additional notices plus the opportunity to opt out.

## The FTC's Safeguards Rule

Any customer information that calls for a dealership's compliance with the Privacy Rule calls for Safeguards Rule compliance, too. The rule is brief, straightforward, and available online.<sup>3</sup> The rule's objective is to protect customers' information by requiring financial institution safeguards that are "reasonably designed to insure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."

<sup>2</sup> "Privacy of consumer financial information," Final Rule, Federal Trade Commission, 16 Code of Federal Regulations, Part 313. To access the text online, go to [www.ftc.gov](http://www.ftc.gov), click on "Legal Resources," click on "Title 16 – CFR," and scroll down to locate part 313, "Privacy of consumer financial information."

<sup>3</sup> "Standards for Safeguarding Customer Information," Final Rule, Federal Trade Commission, 16 Code of Federal Regulations, Part 314. To access the text online, go to [www.ftc.gov](http://www.ftc.gov), click on "Legal Resources," click on "Title 16 – CFR," and scroll down to locate part 314, "Standards for safeguarding customer information."

To make that happen, you must develop, implement, and maintain a *comprehensive information security program*. Your security program must be *in writing* and it must be *readily accessible*. Your security program must contain *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.

## The Elements of Safeguards Compliance

The Safeguards Rule prescribes five elements that you must address in your written, comprehensive information security program. Beyond that, the job of identifying meaningful, concrete security measures falls to the party with the best access to information about your dealership's risks—you. That means that safeguards required for a dealership down the street may not be necessary for you. To accommodate a variety of responses from various businesses, the FTC built flexibility into its compliance requirements.

Here are the five required elements, along with some points to consider in custom-tailoring your compliance efforts.

- (a) **Designate an employee** or employees to coordinate your information security program.

*Coordinate with your coordinator.* Keep your designated security compliance personnel in the loop. If your coordinator is in the IT department, make sure that administrative personnel know to copy your coordinator on any relevant materials, such as service provider safeguards contracts and compliance-related correspondence that arrives addressed to "Dealer-Principal" or "Compliance Officer." If your coordinator is not an IT person, make sure the IT staff knows to forward product and technical announcements to the coordinator. Product information from Reynolds often highlights compliance-support features of the product.

- (b) **Identify reasonably foreseeable internal and external risks** to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
  - (1) Employee training and management;
  - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  - (3) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
- (c) **Design and implement information safeguards** to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

*Focus on the risks that matter—at your dealership.* The Safeguards Rule doesn't demand that you mitigate remote or speculative risks. The FTC recognizes that each business "must focus its limited resources on addressing those risks that are most relevant to its operations." You must identify *reasonably* foreseeable internal and external risks.

And remember that 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. The rule doesn't include a checklist of specific risks to avoid or specific security measures to implement—and there is no blanket rule that forbids you to print out the customer information you need or requires you to install padlocks you don't need. But take note—it's not "reasonable" to leave sensitive customer information out in the open and unprotected.

# Update: Complying with the Gramm-Leach-Bliley Act Privacy and Safeguards Rules

**Prepared for U.S. automotive dealerships  
by Reynolds and Reynolds**

January 2004

(d) **Oversee service providers** by:

- (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
- (2) Requiring your service providers by contract to implement and maintain such safeguards.

Before you send your service provider a safeguards contract, check to see if you already have one. If different parts of your organization are selecting and monitoring service providers, be sure the person designated to coordinate your information security program receives a copy of all service provider safeguards commitments.

And if you are sending out form safeguards contracts, be aware that there is no one-size-fits-all form. The FTC has commented that the Safeguards Rule “should allow financial institutions and their service providers to develop arrangements that do not impose undue or conflicting burdens on service providers that may be subject to other standards and/or agreements concerning safeguards.” Reynolds serves more than 20,000 customers—nearly 90 percent of the automotive retailers and virtually all OEMs doing business in North America. To make it logistically possible to respond to our customers’ requests under the Safeguards Rule, our Safeguards Commitment is available online, integrated into Reynolds’ Master Agreement and Customer Guide. If you have not done so already, please recommend that your information security coordinator read, print, and keep a copy of the Customer Guide by clicking on the Privacy link on [www.reyrey.com](http://www.reyrey.com), and make sure your coordinator is copied on any notice of updates to the Customer Guide.

- (e) **Evaluate and adjust your information security program** in light of the results of the testing and monitoring required by paragraph (c) of this section; 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.

*Keep pace.* “Because of the ever-changing nature of the relevant risks,” the FTC commented, “the Commission does not find it appropriate to delineate risks more specifically within the Rule.” External threats evolve and business environments change, so each dealership must monitor and adjust its information security program. Your security measures must address your dealership’s risks today, not yesterday. Put processes in place to dynamically approach changing vulnerabilities. A slow reaction to changing vulnerabilities will widen the window of opportunity for a successful attack. It’s important to keep pace with both changes in technology and potential threats.

### How is Reynolds responding?

As a service provider to dealership financial institutions, we at Reynolds are doing our part to help our customers comply with the GLB Act. We have an information security management team that monitors industry standards, new technologies, and emerging threats that may affect our customers and our networks. We monitor our service providers. We rely on our customers to tell us what new product features would help their compliance efforts and we provide documentation of the compliance-supportive features of our solutions. And we have incorporated our GLB Safeguards Commitment into the Reynolds Customer Guide—available online along with our Privacy Statement.

### Conclusion

Banks have interacted with customers from behind Plexiglas for years. Automotive dealerships, on the other hand, are new to the role of “financial institution” and operate in unique business environments. Dealership’s customers typically expect to do business in spacious showrooms. Customers are aware that repair shops are literally big enough to drive a truck through—but perhaps not a likely target for identity thieves.

As you respond to the challenge of maintaining safeguards that are appropriate for your dealership, the protections your own customers want, expect, and need from you are key to ensuring their privacy and your compliance—and to protecting your bottom line.

### How to learn more about the Privacy and Safeguards Rules

Please be aware that in addition to the GLB Act, you may also be subject to state and other federal financial privacy regulations. For example, Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”) requires the FTC and banking agencies to implement regulations that will govern how any person who possesses or otherwise maintains consumer information derived from consumer reports should dispose of that information. For more information on the FTC’s Privacy and Safeguards Rules for complying with the GLB Act, you may want to consult these other resources:

*“In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act”*

[www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm](http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm)

*“Financial Institutions and Customer Data: Complying with the Safeguards Rule”*

[www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf](http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf)

*“Safeguarding Customers’ Personal Information: A Requirement for Financial Institutions”*

[www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm](http://www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm)

*“Security Check: Reducing Risks to your Computer Systems”*

[www.ftc.gov/bcp/conline/pubs/buspubs/security.pdf](http://www.ftc.gov/bcp/conline/pubs/buspubs/security.pdf)

The National Auto Dealers Association has also published guidance on complying with the FTC’s Privacy and Safeguards Rules.