"GLB" and What it Means for Auto Dealers

Insights
8.23.17

Developing an information security program is good business, and for auto dealers that are considered "financial institutions" under the Gramm-Leach-Bliley Act (GLB) it is the law. As part of the GLB, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires "financial institutions" to develop a written security plan to protect customer information. Dealers are considered "financial institutions" if they extend credit, facilitate financing through another bank or manufacturer, or provide financial advice or counseling to individuals. Although the Safeguards Rule has been in place since 2003, consumers' heightened awareness regarding data security makes the Rule even more relevant today.

The Safeguards Rule requires "financial institutions" to develop a written security plan to protect customer information. As part of the security plan, each covered dealer must:

- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks of customer information in each relevant area of the dealer's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards and contractually require service providers to implement and maintain such safeguards; and,
- Evaluate and adjust the program in light of the results of the testing and monitoring, or changes in operations or business arrangements.

As the FTC notes, the success of any information security plan depends on the employees who implement it.To help ensure compliance with the Safeguards Rule, dealers should also:

- Check references or conduct background checks (consistent with applicable law) before hiring employees who will have access to customer information.
- Ask new employees to sign agreements to follow the dealership's confidentiality and security standards for handling customer information.
- Limit access to customer information to employees who have a business reason to see it.
- Control access to sensitive information by requiring employees to use strong passwords that must be changed on a regular basis.

- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Train employees to take basic steps to maintain security, confidentiality, and integrity of customer information.
- Regularly remind employees of the dealership's policy and the legal requirement to keep customer information secure and confidential.
- Develop policies for employees who telecommute.
- Impose disciplinary measures for security violations.
- Prevent terminated employees from accessing customer information by immediately deactivating passwords and user names.

Failure to enact a comprehensive information security program poses serious risks, as penalties and costs for non-compliance with applicable laws and regulations are considerable. Other non-tangible risks include damage to a dealer's reputation, loss of customers, and loss of public confidence due to security breaches and the failure to protect sensitive information.

Related People

Melissa A. Dials
Partner
440.740.2108
Email