WHITE PAPER

INTELISYS
a scansource company

What you need to know about the

GLBA Deadline for Automotive Dealerships

Did you know that auto dealerships are subject to compliance with the Gramm Leach Bliley Act (GLBA) because they frequently handle customer financing matters? The Federal Trade Commission (FTC) made amendments to the Safeguards Rule in early 2022 that everyone needs to know.

The amendments go into effect on June 9, 2023, for all GLBA-covered businesses. That means that their information security team needs to be up to speed and ready to implement and ensure solid and consistent compliance.

A Brief GLBA Refresher

Enacted in 1999, GLBA was established as a protective measure to update and modernize the financial industry moving into the 21st century. It requires financial institutions, such as banks, mortgage lenders, and non-financial companies that provide financial lending services to provide customers with clear and accurate information-sharing practices. Ultimately, it allows consumers to opt-out of any interaction if they do not want their sensitive personally identifiable information (PII) shared.

What is the Safeguards Rule?

The FTC's GLBA Safeguards Rule (the rule) took effect in 2003 to protect non-public consumer information (NPI) collected, stored, and used by financial institutions for purposes such as lending and financing. It instructs organizations to implement physical, technical, and administrative protections to protect against phishing schemes, email spoofing, cyber-attacks, and other cybersecurity risks.

This rule applies to all industries that feature a financial component, such as those that offer in-house lending and financial counseling, which includes automotive dealerships. Essentially, the Safeguards Rule provides automotive consumers with all the information the auto dealership collects about them and how it will be collected, used, and stored.

Considering the heavy reliance on technology and the ongoing risk-laden cyber landscape, the FTC regularly updates this rule for consumer protection. In January of 2022, the FTC released Safeguards Rule amendments requiring financial institutions to review, revise, and reinforce measures to protect and secure consumers' NPI to ensure data privacy.

Why Are the GLBA Safeguards Rule Updates and Compliance Vital to Auto Dealerships?

Cybersecurity incidents in the auto industry doubled from 2016 to 2019, up 605%, showing that auto dealerships are as vulnerable to cyber threats as any other industry. Since auto dealerships also offer loans or serve as intermediaries between customers and banks, their customers need to share sensitive NPI for information and loan approval.

Therefore, auto dealers need to remain compliant with the Safeguards Rule for their customers' protection and their business's reputation.

Along with protecting customers' NPI and the auto dealership's reputation, it's crucial to ensure GLBA compliance with the Safeguards Rule to avoid stiff penalties for executives and employees, which include a fine of up to $100,000 per violation. The business's officers and directors might individually incur penalties up to $10,000 and even suffer imprisonment.

The deadline for becoming GLBA Safeguards compliant is June 9, 2023

What Can Auto Dealerships Do to Ensure Compliance with the Safeguards Rule?

The most important aspect of the rule is that it is not as flexible as it once was regarding data security. Everyone will need to understand that it mandates that all financial institutions, including auto dealerships, need to satisfy a substantial list of requirements, regardless of their size, systems, and data they maintain.

Following are five essential tips that auto dealers and their IT/security teams might consider implementing when striving to comply with the new Safeguards Rule.

1. Assign a designated coordinator

This IT professional will be able to implement and review the system and controls to ensure everything is in place for securing data.

2. Obtain a risk assessment

A detailed risk assessment will help auto dealerships identify and mitigate any risks that would leave them vulnerable to non-compliance and threats to customers' PII.

3. Develop and implement Logical Controls

Based on the findings in the risk assessment, the auto dealership must have Logical Controls in place to respond appropriately to those findings. The most common Logical Control used in this capacity is a Managed Detection & Response (MDR) service, providing quick and effective multi-signal visibility, threat containment, and total response to any cyber attacks on the auto dealership's behalf.

4. Appropriate controls with the organization's vendors

Auto dealership clients must work with vendors to work out appropriate contracts, certifications, and future vendor audits, ensuring that they will report any data or systems breach they suffer to the client as soon as they discover issues.

5. Ongoing process for reviewing and updating security controls

Cybersecurity and data threats are not static or predictable, so it's vital that IT teams stay on top of reviewing and updating security controls internally and when working with outside vendors.

How the GLBA Deadline is an Opportunity for Auto Dealerships

Busy auto dealers can easily miss news about important updates and deadlines like those for the GLBA and Safeguards Rule. We feel this critical update is an opportune time to reevaluate your cybersecurity practices, improve data protection policies and be in compliance.

Through Intelisys, you have access to a number of security suppliers that can help auto dealership leaders by providing cyber risk assessments, a virtual chief information security officer (vCISO), Managed Detection and Response (MDR), incident response, security awareness training for staff, and other services.

---

[1] Automotive Buy Sell Report, "Cybersecurity considerations for automotive dealers," October 10, 2018. https://www.automotivebuysellreport.com/cybersecurity-considerations-for-automotive-dealers/

[2] Investopedia, "The Gramm-Leach-Bliley Act of 1999 (GLBA)," February 18, 2022. https://www.investopedia.com/terms/g/glba.asp

[3] Help Net Security, "Automotive cybersecurity incidents doubled in 2019, up 605% since 2016," January 6, 2020. https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/

[4] Esentire, "It's Time to Take Third-Party Risk Seriously," September 3, 2019. https://www.esentire.com/blog/its-time-to-take-third-party-risk-seriously

Sound interesting? Let's talk.

Contact us today to get started!

Michael McCullough

michael.mccullough@scansource.com