ACXIOM

HOW AUTO DEALERS NEED TO PREPARE FOR GRAMM-LEACH-BLILEY ACT AMENDMENTS

By December 9, 2022, automotive dealers must be fully compliant with newly amended regulations set forth under the Gramm-Leach-Bliley Act (GLBA), signaling a significant shift in how automotive dealers use, protect and dispose of customers' data.

Originally passed in 1999, GLBA requires financial institutions to explain their information-sharing practices to their customers while providing safeguards for sensitive customer information. With the advent of the digital age came the compliance requirements necessary to maintaining a consumer's right to privacy.

At the time of GLBA's passing more than two decades ago, the auto industry barely raised an eyebrow, even though the automotive industry has underwritten car loans since 1928.[1] Since then, captive lenders (or finance companies with close ties to car manufacturers) have become the leading auto lender, with most car brands having their own financial arms and some large public dealer groups also establishing captive finance operations. According to Experian's "Q2 2022 State of the Automotive Finance Market report," captive lenders represented 46 percent of loan and lease originations, followed by banks (26 percent) and credit unions (21 percent).

With the pace of digital transformation increasing—and the demand for privacy and security with it—the Federal Trade Commission (FTC) saw a need to amend GLBA to bring automotive dealers into the fold. The new privacy rules apply to automotive dealers who: 1) extend credit to someone (for example, through a retail installment contract) in connection with the purchase of a car for personal, family, or household use; 2) arrange for someone to finance or lease a car for personal, family, or household use; or 3) provide financial advice or counseling to individuals.[2]

The pending compliance deadline and activities needed to prepare appear to be top-of-mind for many automotive dealers, including members of Acxiom's automotive dealer advisory group—automotive dealer CEOs, general managers, sales managers, and fixed operations veterans who offer perspectives on the industry and share challenges and concerns they are facing.

[1] https://lendedu.com/blog/history-of-auto-lending-industry#:~:text=In%201928%2C%20Ford%20set%20up,cars%20were%20bought%20on%20credit
[2] https://www.ftc.gov/business-guidance/resources/ftcs-privacy-rule-auto-dealers-faqs

These are key points gleaned from discussions with members of our automotive dealer advisory group:

- How do we prepare?
- How do we properly store, protect, and dispose of customer data?
- What customer data can be retained after the sale to market services?
- What processes need to be documented?
- Who is responsible for compliance?
- What can I do to defend myself from an FTC investigation?

These have all been areas of curiosity and concern. Automotive dealers are understandably antsy, as even one infraction can result in a $100,000 fine (or worse).

Recently, Acxiom's team of legal and privacy experts, including Chief Privacy Officer Jordan Abbott, shared with members of the automotive dealer advisory group recommendations on how to prepare for the December 9 GLBA compliance deadline.

Here are some of the highlights from that discussion.

DOCUMENT, DOCUMENT, AND DOCUMENT

Simply put, if you fail to document your compliance procedures, then your compliance program may as well not even exist. And while it may seem costly to implement the steps necessary for compliance, not to comply not only leaves you exposed to investigation, but it also puts your customers' private data at risk.

The GLBA amendments require that your automotive dealership develop a written information security program (WISP), which is a bureaucratic way of saying that you need to have a document detailing policies and procedures for how you intend to store and protect confidential data. Your WISP should include both administrative and technical safeguards your organization has in place.

A WISP can be as big and complex as the organization it pertains to. You will find many examples online, though rarely does one size WISP fit all. While there are examples available online that can be customized to fit the needs and size of your organization, Acxiom, a well-practiced manager of data, is also an excellent consultant to help you prepare a WISP.

FORTIFY YOUR CULTURE

When it comes to GLBA compliance, the last mile is the most important, meaning the little things you do can serve you in a big way. You must change the culture of your dealership and hold your entire workforce accountable. Everyone in your organization is an agent of compliance.

Don't leave private information and financial statements open for others to see, whether it's displayed on a laptop or in paper from on a desk. Every computer needs to be password-protected. Make sure your financial office is securely locked when unoccupied. Create a list of privacy protection do's and don'ts for your IT Team.

It is essential that you have a policy and a process—one you can point at to investigators in case a slip-up occurs. Furthermore, you should have a team or at the very least a person in charge of compliance. You needn't invest in a chief information security officer (although that certainly does the job), but you should have a qualified staff member dedicated to implementing your compliance protocols.

THIRD-PARTY VENDORS ARE NOT IMMUNE

"We rely on our DMS," said one advisory group member in the discussion with Acxiom's legal and privacy experts. "If they're not compliant, are we held accountable?"

Simply put, "Yes."

It's very likely that the organization that implements and manages your DMS is well aware of the GLBA amendments. However, you can't afford to make any assumptions. It is up to you to request documentation outlining the steps your DMS provider has taken to encrypt data at rest and in-transit, that it's truncated after a period of time and is securely disposed of at the end of its useful life.

AUTOMOTIVE DEALERSHIPS PARTNERING WITH INSURANCE AGENCIES

Automotive dealerships are increasingly working with insurance companies to market coverage to customers. In some cases, those insurance companies and their agents are physically located inside the showroom. Some of those licensed insurance agents may also be employees of the dealership. It's important to understand what risk and exposure these scenarios might create under the pending GLBA amendments and proactively work to mitigate those risks.

Insurance agencies and their agents are subject to GLBA and have many of the same or similar requirements. However, is the dealership responsible for that insurance company's or its agents' compliance? It depends.

In scenarios where an insurance company and its licensed agent occupy a separate and completely independent office in the showroom as a satellite office unaffiliated with the dealership, GLBA compliance rests with the insurance company and its licensed agents. However, in situations where the licensed insurance agents are also an employee of the dealership, the responsibility for GLBA compliance becomes less clear. It's important to also note that some states, like Virginia, require anyone answering customers' questions regarding insurance marketed and promoted in the showroom also be a licensed insurance agent regardless if the question and the dealership employee providing the answer are affiliated with sales, financing, service, etc. And don't forget, the extended warranties offered during the F&I process and the deal financing are actually insurance policies.

In either scenario—independent satellite office or "employee-agent"—there are some important things dealerships can do to proactively mitigate risk and better comply with GLBA.

- Understand the relationship with an insurance company and its licensed agents operating in your showroom. Are the agents also employees of the dealership? Is there a contract in place? Are the profits shared? If so, how? This is a very fact/subjective standard and not a one-size-fits-all approach. Also, while not addressed specifically under GLBA, ensure you understand state-level requirements for dealership employees discussing insurance options and coverage of policies marketed in the showroom with customers.

- Understand how business resources are shared. Do the agents have access to the same internet, servers, etc. as dealership employees? Can an agent access customer information directly (for instance, on a shared server)?

- Is customer information shared between the dealership and the insurance company and its agents? Are the appropriate permissions from the customer in place before sharing? Is documentation stored on a server that both the dealership and agents have access to or is it just e-mailed? Or is everything completely separated, requiring the customer to complete separate paperwork from the agent?

- Regarding vendor vetting, selection and management, if customer data is being shared, how does the dealership ensure the same level of compliance from the agents? A robust vendor management system would help including contract language and audits. Make sure the agents meet the same level of compliance as the dealership.

PARTING ADVICE

For GLBA compliance, requesting counsel from a respected data manager is always a good route to take. In the meantime, I will leave you with a few parting thoughts to help you feel confident about December 9:

APPOINT A DATA STEWARD. Again, your data steward needn't rise to the level of a chief information security officer, but the individual should be someone dedicated exclusively to the task of compliance.

CONDUCT A DATA INVENTORY. It's important to understand what data you're collecting, the level of its sensitivity and for what purpose you're collecting it.

LIST YOUR PROCEDURES AND POLICIES NOW. Don't wait until December 8. From clean desk policies to password mandates, start developing a program that fits the size and scope of your organization.

STRONGLY CONSIDER STAFF TRAINING. Because every member of your staff is a compliance agent, it is wise to consider mandating compliance and privacy training for your entire workforce.

If you have questions regarding GLBA, data management, privacy, and compliance, feel free to reach out to me. December 9 is fast approaching, and I'm very eager to help.

Steve Schmith serves as Director of Automotive Strategy for Acxiom. *He has more than 25 years of automotive industry experience, including more than 17 years of Big Four experience. He led marketing for Deloitte's automotive practice globally and in the U.S. He also serves as executive director of custom research and data strategy at Automotive News, where he uses his experience with global automotive, manufacturing and consumer research studies to help grow the Automotive News Research & Data Center.*

About Acxiom's Automotive Dealer Advisory Group

Our automotive dealer advisory group includes executives with deep experience in automotive retailing who represent nearly every facet of automotive dealership operations. Throughout the year, Acxiom convenes the group for confidential discussions regarding the products and solutions Acxiom is creating to deliver value to automotive dealers. In those settings, our team of experts also seeks to understand members' challenges and concerns related to digital marketing, ethical use of and protection of customer data, and the evolving regulatory landscape and offer perspectives and advice on tackling those topics. If you are interested in joining Acxiom's automotive dealer advisory group, please contact Steve Schmith at steve.schmith@acxiom.com.

FOR MORE INFORMATION

about our solutions, visit acxiom.com or contact us at info@acxiom.com.

acxiom.com • info@acxiom.com

ACXIOM