Steering Your Auto Dealership into Compliance with New Information Security Rules: A 9-Step Guide

Insights
8.08.22

Auto dealerships that provide financing are subject to the Gramm Leach Bliley Act (GLBA). That's the old news. What's new is that GLBA-covered businesses have until December 9 to implement significant changes to their information security program as required by the recently amended GLBA Safeguards Rule. The updates to the Safeguards Rule are sweeping, and compliance will likely be time consuming and costly. There is, however, a silver lining for dealerships and other financial institutions in a handful of states that have enacted broad consumer privacy laws, such as California, Colorado, Connecticut, Utah, and Virginia. If you're in these states, you don't have to reinvent the wheel. Are you covered by the Safeguards Rule, and if so, what compliance steps should you take?

First, What Is the Safeguards Rule?

The GLBA Safeguards Rule – which first took effect in 2003 – was designed to safeguard non-public customer information collected and held by financial institutions for certain purposes within the scope of the GLBA, including for lending and financing transactions. Not as obvious is the definition of "financial institution" under the GLBA, which includes automotive dealerships that provide financing. So, any consumers who have applied for financing at a dealership in at least the last decade were probably presented with a document that describes what information is being collected, how the information will be used, how it will be protected, and other disclosures. It's the same form consumers get in the mail or electronically every year from their banks, lenders, and other financial institutions.

What Do Dealerships Have to Do by December 9?

In December 2021, the Federal Trade Commission (FTC) revised the Safeguards Rule to require financial institutions to take additional measures to protect and secure customer information. The changes to the rule took effect in January 2022, and the compliance deadline is December 9, 2022. Many financial institutions, however, have been awaiting further guidance from the FTC on the new requirements.

On May 24, 2022, the FTC published a helpful Q&A guide called "FTC Safeguards Rule: What Your Business Needs to Know." This new guide emphasizes the need for financial institutions, including covered dealerships, to "dust off" and revamp their information security program to bring it in line

with emerging security risks and best practices. The FTC's guide identifies nine elements that now must be incorporated into a covered business's information security program. They are listed below along with our commentary and tips for dealerships.

1. **Designate a person who will implement and supervise the dealership's information security program**. The key words here are "implement" and "supervise," which indicate that information security is not just a written policy you set on the shelf and forget about. Rather, there must be active supervision and monitoring to ensure all the protocols are being followed.
2. **Conduct a risk assessment to determine foreseeable risks and threats to the security of customer information**. For dealerships lacking in internal cybersecurity expertise and resources, the best practice is to engage an outside expert to conduct this assessment, as having a fresh set of eyes review your program is better than asking your own security team to evaluate how well they have been protecting the castle. External assessments can also be conducted by or at the direction of legal counsel, which may cost more but gives the added protection of the attorney-client privilege over all confidential communications. Because of quickly evolving cyber risks and technology, consider budgeting to have this assessment done at least every other year, if not annually.
3. **Design and implement the following safeguards to control the risks identified in the risk assessment**:
    - Assess who has access to customer information and reconsider whether they have a legitimate business need for it. This includes identifying whether any third party or vendor is permitted to access the information, including physical (not just electronic) access. If in this review you identify any unjustified access, cut it off.
    - Inventory where your data is collected, stored, and transmitted and on what systems, devices, and platforms. For dealerships that are subject to other state consumer privacy laws, this is one step where you can achieve some economies of scale as you will have to inventory all your data for purposes of compliance with state law. You can apply the same methodology and tools for mapping and inventorying all data, not just customer data that is subject to the Safeguards Rule.
    - Secure customer information by encryption or a similar method.
    - Assess your applications, regardless of whether the company is using a third-party app or has developed its own.
    - Implement multi-factor authentication (MFA) for anyone accessing customer information. MFA is not only a best practice, but many cyber insurance carriers are starting to require it as a condition of writing or renewing cyber policies.
    - Securely dispose of customer information.
    - Develop a method to manage changes to the information system or network.

- Monitor authorized user activity and detect unauthorized user access. Consider investing in new and better tools for endpoint detection and response, or even "managed detection and response" where a cybersecurity firm actually monitors 24/7.

4. **Regularly monitor and test the effectiveness of your safeguards**.
5. **Train staff on security awareness**. How regularly do you remind employees to be vigilant to not click on attachments or links from unknown senders?
6. **Monitor your service providers**. Another way of saying this is to conduct due diligence on the security measures of all vendors that process, collect, store, or access any of your customer data on your behalf or while providing services to the dealership. This involves at least two steps:
    - Proactively reviewing and evaluating the vendor's security measures before engaging the vendor, and if this vendor is already engaged, then conducting an annual or semi-annual security audit or assessment of the vendor's security measures. This can be done by sending a questionnaire or survey to the vendors and requesting documentation, following up if you receive no response, and evaluating their responses to ensure they are adequate to meet your needs. This may include requesting evidence of regular security testing, security certifications (such as SOC 2 or ISO 27001), employee cybersecurity training, and use of basic security protocols, such as MFA, encryption, audit logging and monitoring, and the like.
    - Updating all contracts with vendors that process, collect, store, or access your customer data to address, among other terms:
        1. Prohibiting use, disclosure, and sale of data outside the scope of services provided.
        2. Requiring the vendor to permanently delete the data from their systems either upon the dealership's request or the end of the contractual relationship.
        3. Obligations and liabilities in the event of a data breach, including notification and indemnification obligations.
        4. The vendor's security measures for protecting customer data and an ongoing obligation to maintain those security measures.
        5. Right to monitor or audit the vendor's security measures.
7. **Keep your information security program up to date**. Not to beat a dead horse (who would do that?!), but there is a reason the FTC calls it a "program" and not a "policy." If you treat it like a "policy," then no one will read it and it will sit on the shelf collecting dust and be forgotten like many other legally required written policies. Conversely, a "program" means it's in operation with someone running it. Those not following it must "get with the program." It also means the program is not static and must react and adapt to changes in technology and security risks.
8. **Develop a written incident response plan**. For an incident response plan to be effective, it should identify the response team and their roles and responsibilities in the event of a security breach, as well as the steps to be taken including investigation, remediation, and reporting obligations. Even more important than having a written plan is to practice or have a mock drill, often called a table-top exercise. If your dealership has cyber insurance, have you engaged

often called a table-top exercise. If your dealership has cyber insurance, have you engaged service providers for security breach response that are pre-approved by the insurance carrier? This includes any law firm and forensics vendor that will need to jump in and work with you immediately in the event of a security breach. When disaster strikes, you will not have time for the service providers to run conflicts of interest checks or time to review and sign their contracts and pay their retainers. All of that should be done well in advance of any incident. And if you did not confirm that these service providers are approved by your cyber insurance carrier, you should be aware that the carrier likely will not pay for unapproved providers.

9. **The individual responsible for implementing the security program must report to the Board of Directors at least once per year**. This step suggests that there must be an annual report submitted to the Board providing an update on the security program and any significant developments or security incidents.

The above steps may seem overwhelming, but they can all be done by December 9, 2022, if you take them one step at a time. Seek outside help to fast-track the process. For the most part, most of the cost of implementing these changes will be one-time costs this year. Once you have built the program, including a mechanism for regularly monitoring and updating it, you will not have to rebuild it from scratch every year.

The downside: Many dealerships must comply with two sets of rigorous privacy laws – federal and state. **The upside:** Compliance with the GLBA may support and overlap with compliance efforts under state law, resulting in efficiencies and cost savings.

What Other State Consumer Privacy Laws May Apply to Dealerships?

The new and more demanding GLBA Safeguards Rule is not the only privacy law that auto dealerships must worry about. An increasing number of states have passed comprehensive consumer privacy laws, including California, Colorado, Connecticut, Utah, and Virginia. And each of these states have exempted either all "financial institutions" subject to the GLBA (entity-based exemption) or all data that financial institutions are required by the GLBA to protect (data-specific exemption). Whichever GLBA exemption applies, however, the steps required for compliance with these state laws may overlap and go beyond what the GLBA requires, and dealerships in those states would be wise to utilize a comprehensive approach to all data privacy compliance, not just GLBA compliance.

In California, the California Consumer Privacy Act (CCPA) enhances every California resident's right to know and opt-out-of the collection of their information. However, the CCPA does not apply to data that is subject to the GLBA. Nevertheless, the CCPA does not exempt financial institutions as an entity. Instead, the CCPA exempts the type of data already protected by the GLBA. As a result, there may be people, activities, and information collected by financial institutions that are not covered by the GLBA that are within the reach of the CCPA. For example, the definition of "consumer" is much broader under the CCPA, which deems as consumers several categories of people who interact with

financial institutions, including employees, job applicants, independent contractors, and website visitors.

For dealerships in California that are subject to the CCPA, compliance with the CCPA is equally as important as compliance with the GLBA, especially because the CCPA equips all California consumers with a private right of action for any data breach, and financial institutions are not exempt from this private right of action. Since the CCPA data security requirements appear to be more burdensome than the GLBA Safeguards Rule, if you protect customer data for purposes of CCPA compliance, you will likely have exceeded anything required by the Safeguards Rule.

Where Should You Start?

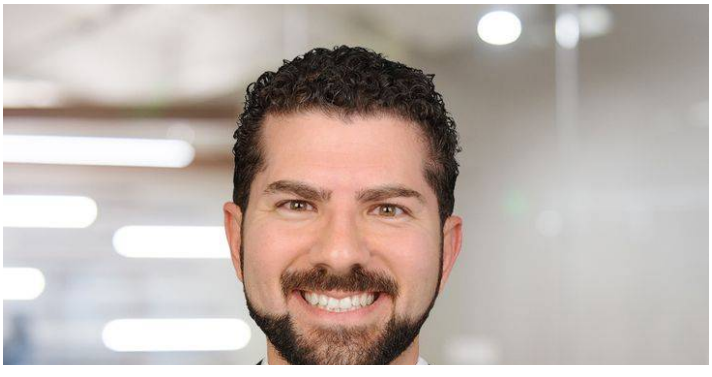
We know that as a dealership, you want to focus on what you do best: sell cars. However, compliance with federal and state privacy laws is a prerequisite to doing so. The deadline to comply with the Safeguards Rule's amendments is quickly approaching and dealerships must begin evaluating whether they are covered, and if so, what needs to be done to come into compliance. We recommend that covered businesses take at least the following initial steps:

1. Designate a person who will implement and supervise the company's information security program;
2. Conduct a risk assessment to determine foreseeable risks and threats to the security of customer information; and
3. Design and implement safeguards to control the risks identified in the risk assessment.

Conclusion

If you are unsure whether your business is covered by – or in compliance with – the Safeguards Rule or any other state or federal consumer privacy law, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on our Consumer Privacy Team or our Automotive Dealership Team. We will continue to monitor developments in this area, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Service Focus

Consumer Privacy Team

Counseling and Advice

Privacy and Cyber

Industry Focus

Automotive Dealership