Published on *The National Law Review* https://natlawreview.com

Gramm Leach Bliley Act: 2 Requirements & 7 Ways to Achieve Compliance

Article By:

Dr. Nick Oberheiden

While the Gramm Leach Bliley Act (GLBA) is now more than 20 years old, it continues to play a central role in how companies collect, process, and store consumers' and customers' non-public information (NPI). GLBA compliance is a key consideration when developing a cybersecurity program, and companies of all sizes must take appropriate measures to ensure that they are adequately safeguarding consumers' and customers' NPI.

While the GLBA does not apply to all companies, its scope is broader than many executives (and many lawyers) realize. This is due primarily to the fact that the GLBA uses the term "financial institution" to describe the entities that are subject to compliance. However, as the U.S. Federal Trade Commission (FTC) explains, the GLBA applies to, "all businesses, regardless of size, that are 'significantly engaged' in providing financial products or services," and this means that many companies that would not normally consider themselves to be "financial institutions" are subject to GLBA compliance.

"Many different types of companies are subject to GLBA compliance. In order to meet their compliance obligations, these companies must adopt policies, procedures, and data security protocols that reflect the unique aspects and risks of their businesses." – Dr. Nick Oberheiden, Founding Attorney of Oberheiden P.C.

What Does the GLBA Require?

The GLBA requires companies that qualify as "financial institutions" to take several affirmative steps in order to prevent the unauthorized collection, use, and disclosure of NPI. It imposes these obligations under two "Rules": (i) the Privacy Rule, and (ii) the Safeguards Rule.

1. The GLBA Privacy Rule

The Privacy Rule establishes financial institutions' obligations with regard to consumer and customer NPI. The GLBA treats "consumers" and "customers" differently, with "consumers" referring to a much larger population of individuals. A "consumer" is anyone who obtains financial products or services from a financial institution, while a "customer" is a consumer who establishes a continuing relationship with a financial institution.

Under the Privacy Rule, financial institutions must provide privacy notices to consumers. They must provide this notice at the time the consumer relationship is established and on an annual basis going forward. In order to comply with the GLBA, a consumer privacy notice must explain what NPI the financial institution collects, how that NPI gets used and shared, and how it gets protected. Crucially, the consumer privacy notice must also provide instructions for how consumers can opt out of having their NPI shared with unaffiliated third parties.

While there are exceptions to the Privacy Rule's notice requirements, financial institutions must be very cautious about not providing privacy notices to consumers. If a financial institution seeks not to provide notice, it must ensure that it can clearly document its qualification for one of the Privacy Rule's exceptions.

2. The GLBA Safeguards Rule

The Safeguards Rule has two main components. It requires financial institutions to implement security protocols (both logical and physical), and it requires financial institutions to provide breach notifications when customers' NPI becomes compromised.

While all financial institutions that collect NPI (which encompasses virtually all financial institutions) must comply with the Safeguards Rule, individual institutions' obligations will differ depending on their resources, the volume of NPI they collect, and the manners in which they use and store NPI. The FTC has provided recommendations for Safeguards Rule compliance; however, it also makes clear that, "[c]ompanies should implement safeguards appropriate to their own circumstances . . . and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network."

What Do Companies Need to Do In Order to Establish GLBA Compliance?

Given the breadth of the GLBA's requirements and the need for each individual financial institution to establish procedures and safeguards that reflect its unique risks and needs, establishing GLBA compliance can present a number of challenges. Companies cannot rely on "off-the-shelf" compliance programs, but instead must develop custom-tailored policies and procedures upon which they can confidently rely to both (i) safeguard consumers' and customers' NPI, and (ii) demonstrate compliance to the FTC when necessary.

With this in mind, some of the key steps that financial institutions must take in order to establish GLBA compliance include:

1. Conduct a Risk and Needs Assessment

As with any corporate compliance effort, the first step toward establishing GLBA compliance is to determine what compliance measures are necessary. This requires an intricate understanding of how the GLBA applies to the company's operations (i.e. when a "consumer" becomes a "customer"), as well as a comprehensive understanding of the company's risks and needs with regard to compliance.

In order to serve its intended purpose, a risk and needs assessment must thoroughly examine all aspects of the company's operations in light of all potential obligations under the GLBA. As a result,

it is important for this process to be conducted by outside counsel with specific experience in the area of GLBA compliance.

2. Adopt Suitable GLBA Compliance Policies and Procedures

With a clear and comprehensive understanding of the company's compliance obligations, the next step is to adopt suitable GLBA compliance policies and procedures. These policies and procedures will need to address numerous issues that will affect virtually all aspects of the company's business. For example, some of the key elements of a GLBA compliance program will include:

- A Corporate Information Security Program
- Assignment of responsibility for compliance to appropriate personnel
- Coordination across all organizational unites with the company
- Internal reporting to company management or the board
- Procedures for management or the board to review reports and oversee the company's information security program
- Ongoing assessment of the risk of unauthorized access to consumer and customer NPI
- Procedures for identifying and ranking information assets according to sensitivity
- Identification of all reasonably foreseeable internal and external threats
- Penetration testing and test result analysis
- Procedures to ensure that system modifications will not negatively impact GLBA compliance

3. Develop a GLBA-Compliant Privacy Policy and Opt-Out System

Beyond developing internal compliance policies and procedures, financial institutions must also develop GLBA-compliant consumer-facing privacy policies and opt-out systems. Here, too, customization is extremely important, as the scope of different companies' needs will vary. Once developed, the company's privacy policy and opt-out system should be submitted to management or the board for approval, and then they should be implemented in all pertinent areas of the company's systems and operations.

4. Implement Suitable Logical and Physical Security Controls

Implementation of suitable logical and physical security controls is one of the foundations of GLBA compliance—and of protecting consumers' and customers' NPI in general. Don't forget, while compliance is important, complying with the GLBA might not necessarily be enough to avoid civil liability in the event of a data security breach. This also underscores the importance of not merely adopting compliance policies and procedures, but also implementing security controls that serve to effectively protect the company.

Here, too, companies' needs will vary widely. Different types of NPI can be more or less attractive to potential intruders, and companies that have substantial resources are generally expected to make proportional investments in their data security protocols. Again, the GLBA does not provide specific guidance, but instead establishes a framework upon which companies must build their own custom-tailored data security programs.

5. Monitor and Enforce GLBA Compliance on an Ongoing Basis

Establishing a compliance program is not a one-time event. Rather, companies must monitor and enforce their compliance programs on an ongoing basis. These efforts should generally be overseen by the company's compliance officer, and the compliance officer should have the authority and resources required to take remedial action as necessary.

6. Document the Company's Ongoing GLBA Compliance Efforts

In addition to developing initial compliance documentation, companies must also document their compliance efforts on an ongoing basis. Not only is this essential for effectively evaluating compliance, but it can also be crucial for demonstrating compliance to the FTC or other authorities.

7. Be Prepared to Execute Breach Notification Protocols When Necessary

Finally, companies that are subject to the GLBA should be prepared to execute breach notification protocols when necessary. Again, while this is an essential component of GLBA compliance, there are other considerations as well. Failure to provide adequate notification to affected consumers or customers can potentially lead to substantial civil liability exposure; and, while complying with the GLBA won't necessarily be sufficient to avoid liability, it can be an important component of a broader defense strategy.

What are the Consequences of Non-Compliance with the GLBA?

When talking about GLBA compliance, it is worth at least briefly mentioning the risks of failure to comply. Under the GLBA, financial institutions can face civil fines of $100,000 per violation, and officers and directors can face personal liability for $10,000 civil fines (also on a per-violation basis). In cases involving intentional violations of the GLBA, financial institutions and their owners and directors can face the possibility of criminal prosecution in federal district court—with criminal fines and imprisonment on the table.

National Law Review, Volumess XI, Number 154