THE
NATIONAL LAW REVIEW

More Companies Must Comply with the Gramm-Leach-Bliley Act, But Don’t Know It. Are You One of Them?

Friday, September 8, 2017

When the topic of data privacy and cyber security comes up, most people automatically think of data breaches, especially given the high-profile nature of so many of them. Breaches and hacks are certainly an issue about which to be concerned, but there are other issues concerning data privacy and cybersecurity that businesses should be cautious regarding as well, such as regulatory compliance. A lot of confusion arises around this area because many businesses do not fully appreciate the specific laws and regulations with which they are required to comply or how to best do so.

For those in the healthcare field, compliance requirements are easily identified. Entities in the healthcare space typically have to comply with HIPAA/HITECH, which means complying with the Privacy Rule and the Security Rule. Entities in the education field have to comply with FERPA and, sometimes, COPPA. But what about other compliance obligations in other industries?

Article By Justin L. Root
Sara H. JodkaDickinson Wright PLLC
Healthcare (Newsletters & Client Alerts)

Communications, Media & Internet
Health Law & Managed Care
All Federal

Take, for example, those in the financial industry, such as banks that have to comply with the Gramm-Leach-Bliley Act (GLBA). Many businesses assume that “financial institution” for purposes of GLBA compliance means a bank and assume that GLBA does not apply to them. This, however, may not be correct. ***GLBA applies to far more businesses than just banks***. The misunderstanding seems to come from two main sources. First, many businesses simply do not understand they are considered to be a “financial institution” under GLBA. Second, many businesses believe they are simply too small to warrant such federal regulatory oversight.

What businesses does GLBA cover?

Businesses that must comply with GLBA are “financial institutions,” but what is considered a “financial institution” goes much further than banks under GLBA. Under GLBA, a financial institution includes businesses that are “significantly engaged” in providing financial products or services, including:

- Check-cashing businesses;
- Payday lenders;
- Mortgage brokers;
- Non-bank lenders;
- Personal property or real estate appraisers;
- Professional tax preparers such as CPA firms; and
- Courier services.

As for the business size requirement, there is none. So, if you are in one of those businesses, there are some things about GLBA you need to know.

Step 1: Complying with the Safeguards Rule

The first compliance hurdle under GLBA is complying with the Safeguards Rule, which was issued by the Federal Trade Commission (FTC), and requires financial institutions to have measures in place to protect and keep secure the consumer information they collect. Interestingly, the Safeguard Rule also applies to credit card reporting agencies and ATM operators that receive information about customers of financial institutions.

Requirement 1: Written Information Security Plan

The first requirement of the Safeguards Rule is that financial institutions must have a written information security plan (WISP) that describes the company's processes for protecting customer information. The WISP should not be one-size-fits-all because it has to include administrative, technical, and physical safeguards appropriate to the business' size, the nature and scope of its activities, and the sensitivity of the customer information at issue. For example, companies have to conduct an assessment of how customers' information could be at risk and then implement safeguards to address those risks. As part of its WISP, each company must do all of the following:

- Designate one or more employees to coordinate its information security program;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the 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, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are flexible, but they are nevertheless *requirements*.

Requirement 2: Securing Information

The Safeguards Rule also requires companies assess and address risks to customer information in all areas of operation, including three areas that are particularly important to information security:

1. Employee Management and Training;
2. Information Systems; and
3. Detecting and Managing System Failures.

There are many different ways to assess and address these various risks, including employee confidentiality agreements, reference checks, need-to-know-only access, password protection, screen locks, ensuring physical security, and other physical and technological safeguards.

Step 2: Complying with the Privacy Rule

Financial institutions must also comply with the Privacy Rule which requires they give their customers a "clear and conspicuous" written notice describing their privacy policies and practices. When the notice is provided and what the notice says depends on what the financial institution does with the information.

Why this matters

The reason this information matters is because the FTC, which enforces GLBA, is doing just that…it is *enforcing* it, especially in the context of data privacy non-compliance issues.

In fact, this issue very recently came up when the FTC settled with TaxSlayer after taking action affecting the company, which offered its customers tax preparation and filing services through its online application. As with all taxes, to prepare and file them, TaxSlayer collected a significant amount of customer data, which essentially rose to the level of personal protected information (PII) under every state's data breach notification statute.

What happened was that in 2015, TaxSlayer was subject to a validation attack wherein a remote attacker gained

access to 8,800 TaxSlayer users. The hackers filed fake tax returns based on the information they collected and had the various tax refunds direct deposited to altered routing numbers.

The FTC investigated the matter and filed a complaint against TaxSlayer for allegedly violating GLBA in a number of ways. First, the FTC alleged TaxSlayer violated the Privacy Rule by failing to provide customers with the required privacy notices. Second, the FTC alleged that TaxSlayer violated the Safeguards Rule by failing to have a WISP in place, by failing to conduct the necessary risk assessment, and by failing to put safeguards in place to control the risk of remote attackers using stolen credentials to steal customer information.

The complaint also alleged that TaxSlayer:

- Failed to require customers to choose a strong password, "which is a standard practice for accounts containing sensitive personal information," instead allowing any password between eight and 16 characters;
- Failed to conduct a risk assessment that would have identified reasonably foreseeable security risks, including those associated with inadequate online identity authentication;
- Failed to use risk-based authentication measures, which allowed hackers to try logging onto multiple different accounts from a remote computer; and
- Failed to validate an email address when the account was first created, meaning they had no reliable way of communicating with customers.

As part of the settlement with the FTC, the company is prohibited from violating the Privacy Rule and the Safeguards Rule of the GLBA for 20 years. Consistent with several past cases involving violations of GLBA, TaxSlayer is required for 10 years to obtain biennial third-party assessments of its compliance with these rules.

The FTC's complaint against TaxSlayer provides a good roadmap of the level of security the FTC expects financial institutions to have under GLBA and what will be expected.

What to do now?

If you are a financial institution, or just discovering that you are one under GLBA, and are not in compliance with the Safeguards Rule and/or the Privacy Rule, whether it be because you don't have a WISP or proper notices, or you are just unsure as to your level of compliance in line with the FTC's standards, please consult one of our data privacy attorneys who can help you review your current compliance status and assist you in checking-off the compliance requirements you must meet.

Source URL: https://www.natlawreview.com/article/more-companies-must-comply-gramm-leach-bliley-act-don-t-know-it-are-you-one-them