WRITING ASSIGNMENT 2

BY: BRYANT WATKINS

NOVEMBER 22, 2024

CYSE 406

Prof: Amanda L. Cheney, Esq.

Memorandum

Date: 11/22/2024

To: Rep. Tito Canduit

From: Bryant Watkins

Subject: How the Gramm-Leach-Bliley Act strengthens cybersecurity in the U.S

What Is This Law?

The Gramm-Leach-Bliley Act was a federal law passed in the United States in 1999 and may also be referred to as the Financial Services Modernization Act of 1999 (iapp.org). The Gramm-Leach-Bliley Act mandates that financial institutions or companies offering consumers financial products and services such as loans, financial/investment advice, or insurance – are to maintain the privacy and security of their customers' sensitive data (FTC.gov). This law was passed following multiple high-profile cases of banks selling consumer information resulting in negative consequences for customers—some of which include credit fraud and identity theft, also in part to seek resolutions to some of the failures leading to the Great Depression (byuh.edu). GLBA was initially introduced by United States Senator Phil Gramm and Representative James Leach – with Representative Tom Bliley also serving as a principal author (byuh.edu).

Gramm-Leach-Bliley Act Cybersecurity Overview

A major component of GLBA is what is called the Safeguards rule. The Safeguards rule is "a regulatory framework that mandates financial institutions to implement comprehensive security measures for protecting customer data", and this rule is of the most importance and relevance to the issue of cybersecurity (saltycloud.com, 2024). There are multiple elements to the

Safeguards rule that must be adhered to, or the institution(s) may face consequences if found to be in violation of.

Element 1 - A qualified individual must be designated as responsible for overseeing and implementing company information security programs as well as enforcing an information security program. (compliancepoint.com)

Element 2 - A risk assessment is required for identifying internal and external risks to customer information security, confidentiality, and integrity (compliancepoint.com).

Element 3 – The institution must then craft and implement controls to address the identified risk from the assessment (compliancepoint.com).

Element 4 – The effectiveness of the institution's controls must be tested and monitored in regular intervals (compliancepoint.com).

Element 5 - Institutions must provide their employees with adequate training that suffices the following requirements: security awareness training tailored to the observed risk identified in the assessment, training is conducted by a qualified information security professional, training program must be up to date to address the current risk climate (compliancepoint.com).

Element 6 - Potential risks from service providers and third-party contractors must be heavily monitored. Ensuring that the party is periodically assessed, maintains sufficient organizational security measures, as well as adherence to specific stipulations set forth in a written agreement (compliancepoint.com).

Element 7 – Institution's information security program must be kept up to date. Organizational security measures be agile and flexible – adjusting measures depending on results on

assessments, penetration testing, traffic monitoring, as well as vulnerability scanning (compliancepoint.com).

Element 8 – A written incident response plan for effective organizational response and recovery following any incident must be crafted. The institution's response plan must include the following: goals, internal processes, hierarchies and roles of authority, communication measures, plan for mitigation of discovered weaknesses, proper internal documentation of incident, and an evaluation as well as revision of incident plan (compliancepoint.com).

Element 9 – The Qualified Individual from the institution must report to the Board of Directors or a senior officer at least once a year. There must be a written report that includes both the overall status of the security program as well as documented materials pertaining to the security program such as incidents, assessments, vulnerabilities, etc. (compliancepoint.com).

Consequences

Failure to adhere to the above listed elements could result in penalties reaching up to $100,000 (compliancepoint.com). A $10,000 fine as well as up to five years in prison is possible for directors and information officers (compliancepoint.com). The consequences are not limited to monetary fines, however. Another consequence that is hard to assign a numerical value to is a tarnished brand or reputation. A damaged brand or reputation could reverberate quickly and last until the institution is able to regain the trust of consumers and prove reliability and security.

Effectiveness

This law proves to possess some effective measures to ensure a secure cyber environment. Adhering to the GLBA Safeguards rule has the potential to enhance trustworthiness

of institutions amongst consumers and customers. Adhering to the GLBA also allows many institutions to remain in compliance with another well-known piece of legislation called the General Data Protection Regulation (GDPR) of Europe. The GDPR is a major information privacy regulation in Europe reaches across the world, so anytime an institution can concurrently comply with that law is an added plus. Adherence to the GLBA also typically leads to less fines as well as possessing higher lifetime value for institutions.

There are some criticisms of the effectiveness of the GLBA, however. The biggest criticism of its effectiveness is the lack of enforcement regulatory capabilities – such as seen with the Health Insurance Portability and Accountability Act. The GLBA also has been ineffective in adapting to the ever-changing landscape of cybersecurity, which includes addressing emerging vulnerabilities. Though it is very imperative to note that the implementation of the GLBA also plays a major role in its effectiveness in safeguarding consumer data.

Conclusion

Overall, this law is one of the more effective ones currently on the books in the United States. While the GLBA has its share of criticisms and weaknesses – it provides an incredible foundation for a further strengthened information security environment at the least. Representative Canduit – this law, and any other variation of it, would prove incredibly beneficial for your constituents. It is certain that many, if not all, of your constituents have ties to financial institutions. Money is ultimately what grabs the attention and urgency of all – for better or worse. Implementing such legislation would showcase to your constituents that you not only are serious about implementing robust cyber security legislation to protect their identity – but you also are serious about coupling that with protection of constituents' financial engagements. If

appropriate actions are taken to further strengthen the GLBA, such as altering it to be better capable of mitigating newer and future threats or vulnerabilities faced by our current landscape, this law could prove to be a real winner for you and your constituents!

REFERENCES

Haley, Steve. “GLBA Cybersecurity Requirements: What Your Organization Needs to Do.” *CompliancePoint*, 18 Aug. 2023, www.compliancepoint.com/cyber-security/glba-cybersecurity-requirements/.

Kranz, Garry. “What Is the Gramm-Leach-Bliley Act?” *TechTarget*, 17 June 2021, www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act#:~:text=Aside%20from%20enhanced%20brand%20reputation,two%20years%20for%2010%20years.

Liu, Katy. “Guide to the Gramm–Leach–Bliley Act.” *Guide to the Gramm–Leach–Bliley Act*, Feb. 2018, iapp.org/resources/article/guide-to-the-gramm-leach-bliley-act/.

Team, SaltyCloud Research. “Understanding the GLBA Safeguards Rule, 2024 Complete Guide.” *IsoraGRC*, 27 Aug. 2024, www.saltycloud.com/blog/glba-safeguards-rule-complete-guide/.

“Gramm-Leach-Bliley Act.” *Federal Trade Commission*, 12 Nov. 2024, www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act#:~:text=The%20Gramm%2DLeach%2DBliley%20Act,and%20to%20safeguard%20sensitive%20data.

“Gramm-Leach-Bliley Act (GLBA).” *BYUH Compliance & Ethics*, compliance.byuh.edu/research-memos/finance/gramm-leach-bliley-act-glba#:~:text=After%20a%20series%20of%20high,Clinton%20on%20November%2012%2C%201999. Accessed 19 Nov. 2024.

"Key Data Privacy and Cybersecurity Laws: United States: Global Data Privacy and Cybersecurity Handbook: Baker McKenzie Resource Hub." *Home*, 29 Dec. 2023, resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/north-america/united-states/topics/key-data-privacy-and-cybersecurity-laws.

Tunggal, Abi Tyas. "What Is the Gramm-Leach-Bliley Act (GLBA)?: Upguard." *UpGuard*, 18 Nov. 2024, www.upguard.com/blog/glba#:~:text=GLBA%20compliance%20is%20a%20requirement,and%20right%20to%20data%20portability.