

Assignment 2.1: Analyzing Cybersecurity Compliance and Enforcement

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

07/07/2025

Introduction

As cyberattacks grow more frequent and complex, protecting consumer data has become an urgent priority across all sectors. Federal agencies, such as the Federal Trade Commission (FTC), and regulations, including the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, play a central role in this effort. They aim to set standards and hold businesses accountable when they fail to meet them. This paper provides a closer examination of how these frameworks impact cybersecurity behavior in practice. Through an analysis of the FTC's handling of the Equifax breach and JPMorgan Chase's approach to GLBA compliance, I'll explore whether current enforcement tools are strong enough or if more robust federal laws are needed to protect consumers in today's digital world.

FTC Enforcement Case Study: Equifax

In 2017, Equifax, a major credit reporting company, experienced a data breach that impacted approximately 147 million individuals. The cause? A known vulnerability in Apache Struts that the company failed to patch, even after receiving warnings. According to the FTC's findings, Equifax also lacked basic security measures, such as proper network segmentation and real-time monitoring (Dad & Nguyen, 2019).

The response from regulators was notable. In 2019, Equifax agreed to a settlement valued at up to \$700 million, covering restitution, state-level penalties, and a federal fine. The company was also required to overhaul its security practices and provide free credit monitoring to those affected.

Despite the size of the settlement, many critics felt it didn't go far enough. The fine represented only a small slice of Equifax's revenue, and no individual executives were held accountable. The company's stock bounced back reasonably quickly. This case highlights both the reach and the limits of the FTC's enforcement authority; it can enforce corrective action, but it lacks the power to impose severe financial consequences or pursue criminal charges (Mireles & Hobaugh, 2024, pp. 36–42).

GLBA Compliance Case Study: JPMorgan Chase

JPMorgan Chase, a global leader in finance, falls under the jurisdiction of the GLBA Safeguards Rule, which requires financial institutions to implement robust protections for customer data. The bank has invested heavily in its cybersecurity infrastructure. Its program includes encryption, 24/7 monitoring, regular penetration testing, and layered access controls, such as multi-factor authentication. JPMorgan also discloses its cybersecurity efforts in corporate reports, showing a level of transparency uncommon in the industry.

Still, the bank has experienced serious security issues. In 2014, it suffered a breach that compromised data belonging to more than 76 million households and 7 million small businesses. The attackers gained access through an employee account that wasn't secured with two-factor authentication. Six years later, in 2020, the Office of the Comptroller of the Currency (OCC) fined the bank \$250 million, not directly for the breach, but for weaknesses in its internal risk management system (Office of the Comptroller of the Currency, 2020).

Since then, JPMorgan has worked to align its practices with the 2021 updates to the GLBA Safeguards Rule. These changes emphasized written security programs, frequent risk assessments, and stronger oversight of third-party vendors (Mireles & Hobaugh, 2024, pp. 66–

75). Although far from perfect, JPMorgan's program shows how a large institution can build resilience by investing in long-term cybersecurity.

Critical Analysis and Recommendations

When comparing these two cases, one significant difference stands out: the FTC tends to get involved only after a breach has occurred, while GLBA compliance is designed to prevent violations from happening in the first place. That's a fundamental gap in the regulatory landscape. Enforcement by the FTC, while important, often feels reactive. Meanwhile, the GLBA only applies to a limited segment of the economy, namely, financial institutions, leaving other sectors without equivalent standards.

The truth is that federal cybersecurity laws, while helpful, don't go far enough. As threats continue to evolve, the regulatory system must keep pace with them. Companies should not view cybersecurity as optional or something to fix only after disaster strikes. Instead, it should be built into their operations from day one. Right now, the financial incentives aren't aligned to make that happen. If the cost of failure remains lower than the cost of compliance, little will change.

Policy Recommendation: Congress should enact a comprehensive nationwide cybersecurity law that applies to all industries. This legislation should establish clear, enforceable standards based on frameworks like NIST SP 800-53 and grant agencies like the FTC the authority to impose fines that genuinely impact a company's bottom line. It should also require public disclosure of significant breaches within a set time frame, 72 hours, for example. These steps would create consistent expectations and give consumers greater confidence that their information is being protected.

Conclusion

Both the FTC and the GLBA Safeguards Rule have shaped how businesses approach cybersecurity, but there are limits to what they can achieve alone. The FTC's handling of Equifax demonstrated the importance of public accountability, even if the penalties weren't severe. JPMorgan's experience showed that even large organizations with sophisticated systems can fall short, and that continuous improvement is essential. Moving forward, a more comprehensive and robust federal strategy is necessary. With the right combination of oversight, incentives, and enforcement, we can close the accountability gap and build a more secure digital future for everyone.

References

Dad, T. K. (Acting), & Nguyen, S. T. (2019, July 22). *Equifax to pay \$575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach*. Federal Trade Commission. <https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach>

Mireles, M. S., & Hobaugh, J. L. (2024). 2–3. In *Principles of cybersecurity law* (2nd ed., Ser. Concise Hornbook Series, pp. 36–75). West Academic.

Office of the Comptroller of the Currency. (2020, November 24). *OCC assesses \$250 million civil money penalty against JPMorgan Chase Bank, N.A.* OCC.gov. <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-159.html>