WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Data Privacy in the Financial Sector: Avoiding a Repeat of First America Financial Corp Scandal

Olumide Ajayi Timothy

Affiliations: Graduate Programs: University of Illinois, Urbana Champaign, University of Cumberlands.
Contact: aolumide26@gmail.com

ABSTRACT

In our modern world, the increased patronage of technology has made the need for strong data privacy regulation imperative than ever before, particularly in the financial sector, where financial institutions manage big data of personal and financial information of their consumers, employees, and partners. The First American Financial Corporation (FAFC) scandal is still treated as one of the biggest financial data security scandals in history. In 2019, the FAFC financial data security scandal exposed 885 million financial and sensitive records due to a relatively minor technological glitch on their website. This issue has led to the loss of consumer trust and confidence in financial technology, making it imperative to avoid a similar problem in the future. This study examines extant financial data security laws, such as the Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act, and Federal Accurate and Credit Transactions Act, amongst other laws.

Objective: The primary aim of this research is to examine the First American Financial Corporation (FAFC) scandal while proffering solutions to avoid similar occurrences in the future.

Method: The theoretical approach is used in this study by analyzing extant legislation, literature, and case studies and recommending how future financial data breaches can be avoided.

Results: The study shows loopholes in the current financial legislative frameworks in the United States of America (USA). It further indicates that, unlike Europe, the USA lacks a centralized data privacy legislative framework.

Conclusion: The study recommends ways to prevent future financial data security breaches in the USA.

Keywords: Financial Data Security, Data Breach, Financial Scandal, The First American Financial Corporation (FAFC), Compliance, Regulations.

Introduction

The financial sector is indispensable to the economic development of any nation, including the United States. The recent technological advancement has caused nations to also transform into the era of financial technology to maintain their global economic position. This transformation has come with concerns, with data breaches and exposure of consumers' financial and sensitive information being a significant concern. Hence, the rising digitization of financial services has made protecting consumers' sensitive information a top priority. Despite considerable cybersecurity and data governance advances, breaches threaten consumer trust and economic stability.

There are various laws regulating the financial industry in the United States, among which are the Gramm-Leach-Bliley Act, which law requires financial institutions to protect consumer privacy; the Fair Credit Reporting Act, which primarily regulates the use of credit reports, identity theft prevention, and other privacy-related practices and the Right to Financial Privacy Act which gives individuals the right to complain about the improper release of information about them in records maintained by financial institutions. Despite these laws and advancements in cybersecurity and data governance, financial data breaches remain prevalent, threatening consumer trust and economic stability.

Surprisingly, in the wake of these unfortunate incidents, the United States lacks a comprehensive data security framework to govern all sectors. Instead, what is obtainable is a plethora of decentralized laws enacted at both the federal and state levels to protect the personal data of US residents in specific areas. (Pittman et al, 2024).

The 2019 FAFC scandal should be treated as a clarion call to ensure data security in the financial markets, which is the focus of this study.

This research will answer the following questions:

1. What are the definitions of keywords in the field of Data Privacy

2. What is the 2019 FAFC Scandal
3. Evaluation of Extant U.S. laws on Financial Data Security
4. What are the lessons to be learned from the FAFC Scandal
5. Recommendation and Conclusions.

Defining the Concepts of Data Privacy

Data means "recorded information, regardless of the form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost, pricing, or management information (Law Insider, 2024).

Data Controller" means the organization determines how information will be processed. Financial institutions collecting information from consumers is a good example. (Swire, P., 2020).

Data Processor" means the individual, businesses, or institutions processing the data information data information on behalf of a data controller. There can be a 3rd party Data Processor on behalf of the Data Controller. (Swire, P., 2020).

Data Subject" means the individual, business, or organization whose data is being processed. A client of a financial institution will fit into this description. (Swire, P., 2020).

Financial Technology refers to institutions that adopt modern technologies to conduct fundamental functions provided by financial services, affecting how users store, save, borrow, invest, move, pay, and protect money.

(McKinsey & Company, 2024)

Personal Information" means information that can identify an individual, business, or research organization and that should be kept confidential. (Swire, P., 2020).

Privacy, simply put, means the "right to be left alone." This definition was introduced by Samuel Warren and Louis Brandeis, published in 1890 in their publication titled "The Right to Privacy" in the *Harvard Law Review*. Hence, privacy is the extent to which people wish to disclose their information to third parties. Privacy can be classified into information, bodily, territorial, and communications (Swire, P., 2020).

Appraisal of the First America Financial Corp Scandal

The New York Times reported, "*First American Financial Corporation, a provider of title insurance, said Friday that it had fixed a vulnerability in its website that exposed 885 million records of mortgage deals going back 16 years. The vulnerability would have allowed anyone access to Social Security numbers, bank account details, driver's licenses, and mortgage and tax records".*

About FAFC: First American Financial Corporation provides title, settlement, and risk solutions for real estate transactions, property data and analytics, title data and technology, home warranty services, and other products and services to real estate professionals, title agents and attorneys, mortgage lenders, homebuilders, and consumers. (FAFC Website, 2024)

The Scandal: In the case of FAFC, the data breach was due to a standard website design error known as Insecure Direct Object Reference (IDOR). Simply put, a link containing sensitive and financial records created for intended recipients was compromised, so anyone with access to that link can view the personal records of FAFC's consumers and use it for fraudulent purposes. The exposed files contained bank account numbers, bank statements, mortgage records, tax documents, wire transfer receipts, Social Security numbers, and photos of driver's licenses, which can be traced back to customers as far back as 2003. This information was accessible without any form of protection. This data breach exposed 885 million sensitive documents, which are detrimental to consumers. (Dellinger, A. J. 2019)

Results of the Scandal: The scandal resulted in investigations by regulatory bodies and class action suits, and FAFC agreed to pay the $1 million fine to New York State.

Appraisal of Financial Data Security Laws in the United States of America

1. The Gramm-Leach-Bliley Act (GLBA): GLBA made significant innovations to data security in the financial sectors. The Act was enacted in response to the merger of U.S. banking, securities, and insurance industries in the late 1990s. The merger of these institutions raised concerns about consumers' data collection and sharing, leading to the birth of GLBA. For instance, the misuse of customer data in the U.S. Bancorp/MemberWorks prompted Congress to include significant privacy and security protections for consumers in GLBA and mandate further rulemaking on privacy and security by the FTC, federal banking regulators, and state insurance regulators. Financial. Institutions were required to comply with GLBA's requirements in 2001 substantially. (Swire, P., 2020).

It is worthy of note that GLBA provisions apply to GLBA applies to all financial institutions, including banks, insurance companies, mortgage lenders, and securities firms, and its provisions are enforced by the Consumer Financial Protection Bureau (CFPB), State Attorneys, Securities and Exchange Commission (SEC), and Federal Trade Commission (FTC). Penalties for noncompliance by financial institutions are over USD 1 million.

Amongst other provisions, GLBA mandates financial institutions to comply as follows:

- To provide a detailed and clear privacy notice to consumers.
- Provide a detailed explanation of the nature of information collected from consumers and how such information is to be shared.
- Provide the liberty for consumers to opt out of sharing their nonpublic personal information with non-affiliated third parties, subject to certain exceptions.
- The appointment of personnel to oversee data protection.
- The Implementation of access controls, encryption, and secure network management.

2. **The Fair Credit Reporting Act (FCRA)**: Credit reports are sensitive information and financial records that consumers would rather keep private. The FCRA was enacted in 1970 to help consumer reporting agencies ensure consumer credit information's accuracy, fairness, and privacy. It is worth noting that FCRA provisions apply to consumer reports agencies (CRA), and their requirements are enforced by the Consumer Financial Protection Bureau (CFPB), State Attorneys, and Federal Trade Commission (FTC). It has the following provisions (Swire, P., 2020).

- CRA agencies must ensure consumer information's accuracy, integrity, and privacy.
- CRAs must allow consumers to access credit reports and correct inaccurate or incomplete information.
- **Users must notify consumers of adverse actions based on their credit reports.**
- Users of Consumer Reports must only use the reports for permissible purposes.
- Based on the report, users must notify consumers when taking adverse actions.
- Users are mandated to implement safeguards for securely disposing of consumer data.
- Financial institutions must also implement programs to detect and mitigate identity theft.

3. The Federal Accurate and Credit Transactions Act (FACTA): FACTA is an improvement to FCRA, enacted in 2003 to introduce new provisions in the interest of the consumers. Some of its relevant provisions are better accessibility to consumer credit information by consumers and consumer protection against identity thefts. It is worth noting that under this Act, the definition of "creditor" excludes attorneys or health providers who extend credit only incidentally.

Also, prior to 2011the Act was enforced by the Federal Trade Commission (FTC) before the responsibility was transferred to the Consumer Financial Protection Bureau (CFPB) in 2011. (Swire, P., 2020). Its key provisions are:

- Consumers have the right to credit reports from major credit reporting agencies.
- To prevent full number disclosure, businesses must truncate credit and debit card numbers on receipts.
- Affords consumers the right to an explanation of their credit scores.
- Organizations must dispose of consumer report information securely to prevent unauthorized access or misuse by burning or shredding physical documents.
- Mandates the destruction of electronic media containing sensitive information.

Another significant provision is the identity theft provisions, also known as the red flag rules. Through these provisions, financial institutions and related organizations can implement identity theft prevention programs to identify "red flags" signaling potential identity theft, develop responses to mitigate identity theft risks and provide regular updates to show evolving threats. (Swire, P., 2020).

The Concept of Preemption

Preemption rights confer on a federal law the right to displace a state law on conflicting provisions. The concept will be applied in the table provided below as it concerns each law.

The Legislative Framework	**Pre-empts State Laws?**	**Additional Provisions**
The Gramm-Leach-Bliley Act **(GLBA)**	Partially	Only to the extent of inconsistencies of such laws. GLBA does not preempt a greater provision

The Fair Credit Reporting Act **(FRCA)**	Partially	Similar to GLBA
The Federal Accurate and Credit Transactions Act **(FACTA)**	broadly preempts state laws concerning consumer reporting and credit data	

Lessons from FAFC Scandals

The FAFC scandals showed that the situation leading to the breach of privacy of millions of people could have been avoided if organizations complied with regulatory frameworks and best data privacy practices.

Conclusions and Recommendations

With the significant significance of the financial sector to a nation's economy, it is crucial to ensure data security and privacy compliance, especially with the advent of modern technologies.

In this study, we recommend as follows:

- **Updated Regulatory Framework**: Desperate times require desperate measures. With the high patronage of technology in the financial industry, there is a need to enact modern laws in line with emerging technologies.
- **Regular Security Testing and Update**: Organizations must adopt a privacy handbook, Policy Manual, or similar internal documents to ensure routine security testing, including code reviews and vulnerability assessments, particularly for custom-developed applications. In FAFC's case, simple URL manipulation led to unfortunate incidents.
- **Hiring Data Privacy and Technology Experts** to conduct breach tests and provide quarterly reports to show vulnerabilities and ensure strong security measures.
- **Mandatory Vendor and Third-Party Risk Management:** Organizations should ensure that 3rd party data processors comply with the data privacy policies to secure consumers' data.
- **Mandatory Timely Incident Response:** Organizations should ensure a timely incident report is made to the data protection officer within the organization for risk management and to the consumers and regulatory agencies within a stipulated period.

References

1. Author Unknown. (n.d.). *First American Title Insurance cyberattack: Impact on the real estate industry*. The Record. https://therecord.media/first-american-title-insurance-cyberattack-real-state-industry
2. California Consumer Privacy Act (CCPA). (2018). https://oag.ca.gov/privacy/ccpa
3. Dellinger, A. J. (2019, May 26). *Understanding the First American Financial data leak: How did it happen and what does it mean?* Forbes. https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/
4. European Union. (2016). *General Data Protection Regulation (GDPR). https://gdpr-info.eu/*
5. Great Place to Work. (n.d.). *Company Overview*. Retrieved from https://www.greatplacetowork.com/certified-company/1243853#:~:text=Company%20Overview&text=We%20offer%20title%20insurance%2C%20settlement,mortgage%20lenders%2C%20homebuilders%20and%20consumers.
6. McKinsey & Company. (n.d.). *What is fintech?* McKinsey & Company. Retrieved December 4, 2024, from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-fintec
7. National Institute of Standards and Technology (NIST). *Cybersecurity Framework.*
8. New York State Department of Financial Services. (2019). *Cybersecurity Regulations for Financial Institutions.*
9. Pittman F. P., Hafiz A. & Hamm A (White & Case LLP),(2024), Data Protection Laws and Regulations USA 2024, Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
10. Pittman F. P., Hafiz A. & Hamm A.,(2024), Data Protection Laws and Regulations USA 2024, Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
11. Statista. (2024). *Most significant data breaches in the financial sector worldwide from 2008 to 2024*. Retrieved from https://www.statista.com/statistics/1323568/largest-data-breaches-in-financial-sector-

worldwide/#:~:text=All%2Dtime%20biggest%20financial%20data%20breaches%20worldwide%202024&text=Between%202008%20and%202024%2C%20the,million%20financial%20and%20personal%20records

12. Swire, P., & Kennedy-Mayo, D. (2020). *Law and Practice for Information Privacy Professionals* (3rd ed.). International Association of Privacy Professionals.
13. Warren, S., & Brandeis, L. (1890, December 15). The right to privacy. *Harvard Law Review*, 4(5), 193–220. Retrieved June 4, 2021, from https://archive.org/details/Harvard_Law_Review_v4
14. Zengler, T. (2019, May 24). *Data Leak Exposes Millions of Documents on Real Estate Deals*. The New York Times. Retrieved from https://www.nytimes.com/2019/05/24/technology/data-leak-first-american.html