Studies in Social Science Research
ISSN 2690-0793 (Print) ISSN 2690-0785 (Online)
Vol. 3, No. 4, 2022
www.scholink.org/ojs/index.php/sssr

Original Paper

A Simulation of How a Cloud Service Provider from the Midwest Should Behave When Faced with a Potential Cyber-Attack, Where Many of Its Customers Do Business in the Healthcare, Banking, and Educational Industries

Donald L. Buresh, Ph.D., Esq.[1]

[1] Touro University Worldwide, United States

Received: September 9, 2022 Accepted: September 22, 2022 Online Published: September 28, 2022

doi:10.22158/sssr.v3n4p24 URL: http://dx.doi.org/10.22158/sssr.v3n4p24

Abstract

This essay aims to explain to the senior management of a company what must be accomplished to be compliant with federal sectoral privacy laws. It is a byzantine maze of pitfalls where a single cyber-attack can lead to extensive oversight by the Federal Trade Commission. The path taken by this paper is that a cloud computing provider should implement the most stringent security framework in existence that encompasses the myriad number of privacy laws in the United States. The reason is that vigorously embracing a strict standard makes a firm likely to comply with the various sectoral privacy laws. However, suppose a company is cyber-attacked and has the misfortune of being prosecuted by the Federal Trade Commission. In that case, the article suggests that the firm take a mature approach to the litigation, not complaining to the agency that it is the victim. A mature approach to federal oversight might lessen the time of the supervisory period. By admitting security omissions and commissions and robustly accepting regulatory guidance, a firm can proceed in conducting its business, not fretting over the de facto guardianship by the Federal Trade Commission.

Keywords

California Consumer Privacy Act, California Privacy Rights Act, Federal Trade Commission, FedRAMP Security Framework, Illinois Biometric Information Privacy Act, In the Matter of TaxSlayer, LLC

Introduction

This article discusses how a Chief Privacy Office (CPO) of a Midwest-based multinational corporation that offers various cloud, mobile applications, and artificial intelligence solutions to other corporations on the planet would explain the federal sectoral privacy requirements to senior management. The American sectoral approach to privacy is a byzantine maze of laws with few overreaching principles. The federal privacy laws in the United States are not comprehensive or consistent. A corporate approach to privacy must thus adhere to policies that ensure a corporation is compliant with a wide range of privacy laws so that it is unlikely to become embroiled in litigation.

While no corporation is immune from a cyber-attack, companies can learn from other organizations that have come under scrutiny by the Federal Trade Commission (FTC). The case explained in this essay is *In the Matter of TaxSlayer, LLC*.[1] Numerous cases could have been selected, but *TaxSlayer* demonstrates quite vividly the adverse effects of an FTC suit. Essentially, a company that has the misfortune of being prosecuted by the FTC will typically be subordinate to the FTC for at least 20 years, filing report after report ensuring that it complies with the applicable privacy laws. This is a difficult situation to be in, where the purpose of a business may be transformed from maximizing profits to complying with FTC requirements.

The path to compliance is littered with the corpses of defunct corporations that are longer in business. The pitfalls are legion. There is no concise way to explain how the FTC can construe that an organization has violated privacy law. A company must strictly comply with the relevant privacy laws or otherwise be accused and convicted of deceptive practices. There is no royal road to compliance. It is sometimes an all-or-nothing affair, where the slightest misstep may precipitate an FTC suit. The goal is to obey all privacy laws all the time or be resigned to continuously defending oneself in court. There is no other way.

Federal Risk and Authorization Management Program

Suppose the company is a multinational corporation offering various cloud, mobile applications, and artificial intelligence solutions to other corporations around the globe. The firm should likely comply with the Federal Risk and Authorization Management Program (FedRAMP). The federal program provides a standardized approach to security authorizations for cloud services.[2] Various federal agencies govern FedRAMP within the Executive Branch. These agencies work collaboratively to develop, manage, and operate FedRAMP. These agencies include:[3]

---

[1] *In the Matter of TaxSlayer, LLC*, Complaint Docket No. C-2646 (n.d.), *available at* https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf.

[2] FedRAMP Staff, *Governance*, FEDRAMP (n.d.), *available at* https://www.fedramp.gov/governance/.

[3] *Id.*

- Office of Management and Budget;
- Joint Authorization Board;
- National Institute of Standards and Technology;
- Department of Homeland Security;
- Federal Chief Information Officers Council; and
- FedRAMP Program Management Office.

The National Institute of Standards and Technology (NIST) advises FedRAMP on the Gramm-Leach-Bliley Act (GLBA) compliance and assists in generating standards for the accreditation of independent third-party assessment organizations (3PAOs).[4] NIST's responsibility is to ensure that FedRAMP possesses the security controls that support a supply chain cybersecurity risk assessment program.[5] In particular, NIST ensures that FedRAMP complies with NIST Special Publication 800-161 standard.[6] The security controls for NIST SP 800-161 are:[7]

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Personnel Security
- Provenance
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Because the company has customers in the healthcare, banking, and higher education sectors, the security controls may be different for these customers. The Chief Privacy Officer (CPO) ensures that the cloud, mobile applications, and artificial intelligence solutions comply with the security frameworks for each sector. The healthcare, banking, and higher education sectors will be discussed in turn.

[4] Jon Boyens, Celia Paulsen, Hatha Systems, & Nadya Bartol, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (Apr. 2015), *available at* https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08

[5] *Id.*

[6] *Id.*

[7] *Id.*

Healthcare Industry Issues

The security framework for the healthcare sector is subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996.[8] HIPAA is a mandatory federal framework for the healthcare sector. The law applies to covered entities, such as health plans, health care clearinghouses, and health care providers, who conduct certain financial and administrative transactions electronically.[9] Because the firm presumably contracts with healthcare providers, HIPAA likely applies to the firm through a business associate agreement (BAA). HIPPA's Privacy Rule addresses privacy, disclosures, access, and reporting.[10] The law also possesses a Security Rule that protects electronic health information.[11] The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009 and addressed the security concerns regarding the transmission of health information.[12]

The company should be HIPAA compliant because the firm is a third-party business associate of corporations in the healthcare industry. The compliance includes satisfying the legal requirements of the HIPAA Privacy Rule and Security Rule. The company should also be HITECH compliant because it is likely involved in transmitting personal healthcare information.

Banking Industry Issues

Because the company does business with corporations in the banking sector, it is likely to be concerned with several financial industry security frameworks. First, the Federal Financial Institutions Examination Council (FFIEC) framework may be an issue for the company.[13] The FFIEC is mandatory for federally chartered financial institutions. Although no certification is available, a financial institution can be audited for sufficiency. Given that the firm provides cloud, mobile app, and Artificial Intelligence (AI) services to organizations in the banking sector, the company may become involved when one of its customers is audited.

---

[8] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CENTERS FOR DISEASE CONTROL AND PREVENTION (N.D.), *available at* https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] HHS Staff, *HITECH Act Enforcement Interim Final Rule*, UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES (n.d.), *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

[13] *Welcome to the Federal Financial Institutions Examination Council's (FFIEC) Web Site*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (Nov. 9, 2021), *available at* https://www.ffiec.gov/

Banks routinely deal with ATM and credit card information. The Payment Card Industry Data Security Standard (PCI-DSS), first published in 2004, is not a regulation, but PCI-DSS obligations flow from merchant agreements or brand licensing.[14] The PCI-DSS collaborates with credit cards, such as Visa, MasterCard, American Express (AMEX), Discover, and the Japanese Credit Bureau (JCB).[15] The PCI-DSS applies to merchants, banks, and organizations engaged in financial processing.[16] The framework aims to protect cardholder data using 12 requirements and over 200 sub-controls.[17] Several states, such as Nevada and Washington, have incorporated the PCI-DSS into laws. Self-assessment and certification are available.[18]

The Control Objectives for Information and related Technology (COBIT) was developed in 1996 by the Information Systems Audit and Control Association (ISACA) to ensure that the financial audit community adequately addresses IT-related environments.[19] COBIT is predicated on principles that describe the core requirements of a governance system for corporate information and technology and the enterprise as a whole.[20] COBIT can involve information technology (IT) management beyond security, such as storing data on a cloud.[21] COBIT possesses six governance system principles, three governance framework principles, and 13 IT alignment goals.[22] Software developers typically use COBIT in the financial services industry.

All three frameworks should be of interest to the company. These security standards may impact the firm because its customers may be required by law, regulation, or customs to adhere to them. The company should ask its banking and financial sector customers about the applicable compliance standards. Then, the corporation should evaluate its security framework and standards to ensure that the firm satisfies the needs of its banking industry clients.

---

[14] *Official PCI Security Standards Council Site*, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (2022), *available at* https://www.pcisecuritystandards.org/

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] Katie Terrell Hanna, *COBIT*, TECH TARGET (Sep. 2021), *available at* https://www.techtarget.com/searchsecurity/definition/COBIT#:~:text=COBIT%20is%20the%20acronym%20for,business%20risks%20and%20control%20requirements

[20] *Id.*

[21] *Id.*

[22] *Id.*

Higher Education Issues

The Family Educational Rights and Privacy Act (FERPA) is likely to be the federal law that affects the firm's higher education customers. FERPA requires federally funded educational institutions under the United States Department of Education to comply with the law to protect student data.[23] FERPA gives parents and students after they reach 18 years old, the right to inspect and review their records, as well as the right to request the school to correct records that are inaccurate or misleading.[24] FERPA also permits schools to release student records, provided they have received written permission from a parent or eligible student.[25] However, FERPA does permit schools to disclose student records without consent to:

- School officials with a legitimate educational interest;
- Other schools for which a student has transferred;
- Specific auditors or evaluators;
- Parties associated with financial aid to a student;
- Organizations conducting research for or on behalf of a school;
- Accrediting organizations;
- Judicial orders or lawfully issued subpoena;
- Officials involved in health and safety emergencies; and
- State and local juvenile justice system authorities, according to State law.[26]

The company may be responsible for storing student records. It should ensure that either the individual requesting student records has consent from a parent or the student who is 18 years or older or satisfies one or more of the exceptions above.

State Privacy Laws

In this section, the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), and the Illinois Biometric Information Privacy Act (BIPA) will be discussed. The subsections will describe the various state laws and their implications.

California Consumer Privacy Act

State privacy law is in a state of flux. The state privacy landscape is changing daily. The CCPA, as amended by the CPRA, was the first comprehensive state privacy law.[27] Currently, Colorado and

[23] *Family Educational Rights and Privacy Act (FERPA)*, UNITED STATES DEPARTMENT OF EDUCATION (Aug. 25, 2021), *available at* https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECHNOLOGY LAW

Virginia have also passed comprehensive privacy laws.[28] Maine and Nevada have privacy laws on the books, but the statutes are not nearly as comprehensive as the CCPA.

On June 28, 2018, the CCPA became law.[29] Amendments to the CCPA were passed on August 31, 2018, and the CCPA became effective on January 1, 2020.[30] The CCPA defines a California resident domiciled to be a California consumer.[31] There is no protection for personal information temporarily located within California.[32] The CCPA posits that a California resident has the right to know the classes of personal information collected, the source, and what entities are purchasing that information.[33] California residents also have the right to review the personal information collected.[34] Finally, California residents can rightfully request that their personal information be deleted.[35]

The CCPA has seven critical provisions. First, California consumers have the right to opt-out of having their personal information sold.[36] Second, covered businesses cannot charge California residents a high price when they exercise their rights.[37] Third, California consumers are entitled to an electronic copy of their data that is easily transferable.[38] Fourth, for individuals under 16, parents or guardians must permit a data collection company before data can be collected.[39] Fifth, a company doing business in California must disclose the categories, recipients annually, and sources of all data it collects, stores, discloses, or sells.[40] Sixth, a corporation's website must have a link entitled "Do Not Sell My Personal

---

JOURNAL 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/

[28] *Id.*

[29] Donald L. Buresh, *A Comparison Between the European and American Approaches to Privacy*, 6 INDONESIAN JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 2, 253-281, (2019), https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=

[30] *Id.*

[31] Donald L. Buresh, *supra* note 27, at 270.

[32] *Id.*

[33] Donald L. Buresh, *supra* note 27, at 270.

[34] *Id.*

[35] *Id.*

[36] Rodgin Cohen, John Evangelakos, Nader Mousavi, Matthew Schwartz, & Nicole Friedlander, *Sullivan & Cromwell Discusses California Consumer Privacy Act of 2018*, THE CLS BLUE SKY BLOG, (July 23, 2018), https://clsbluesky.law.columbia.edu/2018/07/23/sullivan-cromwell-discusses-california-consumer-privacy-act-of-2018/

[37] *Id.*

[38] Donald L. Buresh, *supra* note 27, at 271.

[39] Rodgin Cohen et al., *supra* note 36, at 5.

[40] Donald L. Buresh, *supra* note 27, at 271-72.

Information" so California residents can exercise their right not to sell their personal information.[41] Finally, an organization doing business in California must specify two methods where a consumer can ask for their personal information.[42]

There are two kinds of non-compliance penalties. First, there are penalties due to security breaches. The damages are at most $750 per violation or the actual damages, whatever is the larger amount.[43] The Attorney General of California may enforce the law's privacy provisions via civil penalties with a maximum of $7,500 per violation.[44] For example, if a data breach involves one million individuals at $750 per violation, the maximum penalty would be $750 million. If the California Attorney General decides to sue, the maximum penalty would be $7.5 billion.[45] Thus, the maximum penalties under the CCPA could be well beyond the financial reach of many organizations.[46]

California Privacy Rights Act

The CPRA enhances the CCPA.[47] The threshold for the number of consumers or households was increased to 100,000. It now applies to businesses that receive 50 percent or more of their annual revenue from selling or sharing consumer personal information.[48] The CPRA permits California consumers the right to opt out of automated decision-making technology that is associated with a consumer's economic situation, health and personal preferences, location or movements, and work performance. The CPRA also strengthens the opt-out rights for minors.[49] The CPRA defined *sensitive personal information*, such as *biometric or health information*, the content of non-public information (i.e., email and text messages), ethnicity, *genetic data*, race, religious or philosophical beliefs, sex life, or sexual orientation information, and union membership. Under the CPRA, sensitive personal information has stringent consent, disclosure, opt-out requirements, and purpose limitations.[50]

The CPRA grants consumers the right, subject to some exceptions, to demand the deletion of any consumer personal information purchased or sold.[51] Consumers have the right to correct erroneous

---

[41] *Id.* at 272.

[42] Rodgin Cohen et al., *supra* note 36, at 3.

[43] Donald L. Buresh, *supra* note 27, at 272.

[44] *Id.*

[45] Rodgin Cohen et al., *supra* note 36, at 6.

[46] Donald L. Buresh, *supra* note 27, at 273.

[47] *CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Operations*, WIREWHEEL, INC., 2 (2020), https://wirewheel.io/resources/cpra-ccpa-gdpr-impact-on-data-privacy-operations/

[48] *Id.*

[49] *Id.* at 3.

[50] *Id.* at 4.

[51] *Id.* at 5.

information and restrict the use and disclosure of sensitive personal information.[52] Consumers now have the right to access the decision-making logic used in collecting, storing, disseminating information, and describing the likely outcomes of the process.[53] Consumers may request that the business transmit specific personal information to third parties when technically feasible.[54] The CPRA requires a company to perform an annual cybersecurity audit and submit personal information processing risk assessments.[55]

The CPRA limits the collection, storage, use, and retention of personal information based on the desired end of collecting the data.[56] The fine increased to $7,500 per violation involving individuals under 16.[57] The 30-day cure period after a breach was removed.[58] The CPRA expanded the consumer privacy right of action so that violations of email accounts were covered.[59] The CCPA with the CPRA looks much like the GDPR regarding various criteria.[60]

Illinois Biometric Information Privacy Act

BIPA is a comprehensive privacy law passed in 2008. BIPA jumped into the privacy arena when the Illinois Supreme decided *Rosenbach*.[61] Under *Rosenbach*, a fourteen-year-old boy went on a field trip to Six Flags Great America in Gurnee, Illinois.[62] His mother purchased a ticket for her son online.[63] When entering Six Flags, the child was required to scan his thumbprint to verify his identity and activate his season pass but did not receive any paperwork describing the reasons why the thumbprint scan was taken nor how the biometric data would be used.[64] When the child returned home, he told his mother about the scan print.[65] Six Flags did not send the child or his mother a consent form regarding

[52] *Id.*

[53] *Id.* at 6.

[54] *Id.* at 7.

[55] *Id.* at 8.

[56] *Id.*

[57] *Id.* at 9.

[58] *Id.*

[59] *Id.*

[60] *Id*.

[61] Rosenbach v. Six Flags Entertainment Corp., 129 N.E.3d 1197 (Ill. 2019); *see also* Chloe Stepney, *Actual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law*, 40 LOY. LOS ANGELES ENT. L. REV. 51 (2019).

[62] *Rosenbach*, 129 N.E.3d at 1200.

[63] *Id.*

[64] *Id.*

[65] *Id.*

taking a scan of the child's thumbprint.[66] Six Flags did not share its policy regarding its biometric information storage policies with the plaintiffs.[67]

In *Rosenbach*, the Illinois Supreme Court found a technical violation of BIPA. There was no showing of actual damages that gave rise to a cause of action.[68] However, the Court employed the statute's plain meaning, opining that a plaintiff's standing under BIPA is not controlled by actual harm but rather by an infringement of a statutory right, which gave rise to the cause of action.[69] The decision of the Court was unanimous.[70]

Lessons Learned from the State Privacy Laws Evaluated

The CCPA, CPRA, and BIPA pose many issues for a company. The CCPA, as amended by the CPRA, makes doing business in California much like doing business in the European Union, a highly regulated activity. The reason is that the CCPA plus the CPRA looks similar to the General Data Protection Regulation (GDPR). Although the CCPA is an enforceable law, the CPRA is effective on January 1, 2023.[71] This information is good news for a firm because there is time to prepare for CPRA compliance.

Under BIPA, a company may be sued under Illinois law when only a technical violation happened, and no actual damages were incurred. If customers store biometric data on a company's cloud, the firm may be liable under BIPA, possibly because the firm is domiciled in the Midwest, a neighbor of the State of Illinois. It is likely that many of the firm's customers are based in Illinois or do a significant amount of business in Illinois. Either way, a company should pay particular attention that it does not intentionally or inadvertently violate BIPA. It should be duly noted that BIPA permits private action, which increases the likelihood of litigation. For Texas and Washington, the two other states with biometric privacy laws, only the state's Attorney General can institute an action against a defendant.[72]

---

[66] *Id*.

[67] *Id.*

[68] *Id.* at 1202.

[69] *Id.* at 1206.

[70] *Id.* at 1207.

[71] *California Privacy Rights Act: An Overview*, PRIVACY RIGHTS CLEARINGHOUSE (December 10, 2020), https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,personal%20information%20to%20third%20parties.&text=The%20California%20Privacy%20Rights%20Act%20expands%20this%20to%20cover%20data,includes%20a%20username%20and%20password

[72] Donald L. Buresh, *supra*, note 13.

Federal Trade Commission v. TaxSlayer

This section presents the TaxSlayer case as an example of how the FTC enforces privacy violations. The penalties imposed by the FTC in *TaxSlayer* were similar to those imposed in other cases. Thus, it makes sense only to discuss *TaxSlayer*.

History of the TaxSlayer Case

TaxSlayer is a Georgia limited liability corporation that advertises, offers to sell, sells, and distributes various products online, including an online tax return preparation service, TaxSlayer Online, and an electronic filing service.[73] The business began over 50 years ago when it was only a tax preparation business. In the 1980s, the company created in-house tax preparation software; in the 1990s, the firm developed a browser-based version. In the succeeding 30 years, the organization offered a mobile tax preparation app. The FTC stated that the complaint was based on the browser-based software service and the mobile app.[74]

In 2016, over 950,000 individuals filed their tax returns via TaxSlayer Online.[75] The software permitted users to create an online account by entering a username and password on a login window. The user proceeded to input their personal information, such as social security number, telephone number, annual income, marital status, and other information necessary to file federal and state tax returns.[76] After the required information was entered, TaxSlayer Online prepared customer income tax returns, allowing customers to file their returns electronically and receive any refunds in their bank accounts or debit card.[77]

Issues before the FTC

According to the FTC complaint, TaxSlayer was a financial institution subject to Section 509(3)(A) of the GLBA, 15 USC § 6809(3)(A) because it offers tax planning and tax preparation services.[78] The company gathered non-public personal information as it is defined by 16 CFR § 313.3(n) and 12 CFR § 1015.3(p)(1)-(3).[79] Because of these two reasons, TaxSlayer was subject to the GLBA Privacy Rule and Safeguards Rule.

Violations of the Privacy Rule

The FTC complaint observed that covered financial institutions were required by law to deliver initial and annual privacy notices to their customers that must be clear and conspicuous.[80] The privacy notice

[73] *In the Matter of TaxSlayer, LLC*, *supra*, note 1.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] See 16 C.F.R. § 313.3(b) and 12 C.F.R. § 1016.4 and 1016.5.

must contain specific information, including the classes of non-public personal data that were collected and disclosed, the types of data that third parties could receive from TaxSlayer, and the security, confidentiality, and integrity policies of the organization.[81] The complaint opined that TaxSlayer was required to provide its privacy notice so that consumers reasonably expect to receive the notification.[82] According to the FTC complaint, TaxSlayer failed to provide its consumers with a clear and conspicuous privacy notice.[83] The FTC did acknowledge that the privacy notices that TaxSlayer did give its customers were near the end of its License Agreement. The privacy notice was not conspicuous and did not stress the importance, nature, or relevance of the company's privacy policy to its customers.[84]

Violations of the Safeguards Rule

According to the FTC complaint, the purpose of the Safeguards Rule is:

"[T]o protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive information security program that is written in one or more readily accessible parts, and that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue."[85]

The Safeguards Rule required that a financial institution (1) designate at least one person to manage the firm's information security program, (2) identify reasonably foreseeable risks that affect the security, confidentiality, and integrity of customer information, (3) design and implement information protections to control the identified risk through a risk assessment process, while regularly testing and monitoring the effectiveness of the protections in place, (4) oversee service providers and vendors so that they are also protecting the confidentiality, integrity, and availability of customer information, and (5) evaluate and change the information security program in light of relevant evolving circumstances.[86]

The FTC complaint asserted that TaxSlayer did not possess a written information security program until November 2015, approximately six years after the GLBA became law.[87] Second, TaxSlayer did not conduct a risk assessment analysis, which could have identified internal and external risks to

[81] See 16 C.F.R. § 313.6 and 12 C.F.R. § 1016.6.

[82] See 16 C.F.R. § 313.9 and 12 C.F.R. § 1016.9.

[83] See 16 C.F.R. § 313.4 and 12 C.F.R. § 1016.4.

[84] *In the Matter of TaxSlayer, LLC*, *supra*, note 1.

[85] *Id.*

[86] *Id.*

[87] FTC Staff, *Gramm-Leach-Bliley Act*, FEDERAL TRADE COMMISSION, (n.d.), *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (Here, according to the FTC, the Act became law on November 12, 1999).

customer information security, confidentiality, and integrity.[88] Third, TaxSlayer did not require the consumer to select strong passwords consisting of capital and small letters, numbers, and special characters and failed to implement risk-based authentication measures that may have prevented a cyber-attack.[89] TaxSlayer failed to inform users when a customer's mailing address, password, security question, bank account routing number, or refund payment method changed.[90] TaxSlayer did not demand that customers validate their email addresses when customer accounts were created and did not employ "readily available tools" that prevented devices and IP addresses from being hacked.[91]

TaxSlayer was the victim of a list validation cyber-attack that began on October 10, 2015, and lasted until December 21, 2015, when the company instituted multi-factor authentication.[92] Because of the list validation cyber-attack, hackers gained full access to 8,882 existing TaxSlayer accounts. TaxSlayer was not aware of the cyber-attack until January 11, 2016, approximately three weeks after the cyber-attack ended. The cyber-attack was discovered when a customer alerted TaxSlayer that suspicious activity was occurring on their account.[93] The FTC complaint observed that customers spend significant time resolving cyber-attack outcomes. Customers who are victims of identity theft may have to obtain a new personal identification number (PIN) from the Internal Revenue Service (IRS) and wait months for their tax refunds.[94] Customers may also have to monitor their credit reports for fictitious or false information being listed on their reports and possibly suffering substantial financial losses.[95]

Resolution of the TaxSlayer Case

On October 20, 2017, *TaxSlayer* was decided by the FTC.[96] The agency enjoined TaxSlayer from violating any provision of the Privacy Rule and the Safeguards Rule. TaxSlayer was required to obtain biennial cyber-risk assessments and reports from a qualified, objective, and independent third-party employing accepted cyber-risk procedures and standards. Each assessment must contain specific administrative, physical, and technical safeguards instituted by TaxSlayer, which were appropriate for TaxSlayer's size, and complexity. The protections must address the nature and scope of TaxSlayer's

---

[88] *In the Matter of TaxSlayer, LLC*, *supra*, note 1.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *In the Matter of TaxSlayer, LLC*, Decision and Order Docket No. C-2646 (October 20, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_decision_and_order.pdf

activities and the sensitivity of guarded customer information.[97] TaxSlayer was also required to demonstrate that the precautions met or exceeded the defenses demanded in Section I (B) of the Order.[98] TaxSlayer was ordered to certify that its security program was sufficiently effective to assure customer information security, confidentiality, and integrity during the reporting period.[99] The FTC stated that when the assessment report was done, the report should be submitted to the FTC.[100]

TaxSlayer was required to acknowledge receipt of the Order within ten days of its effective date. For 20 years after that, deliver a copy of the Order to the company's officers, directors, managers, members, employees, agents, representatives having managerial responsibilities, and any business entity resulting from a change in compliance reports and notices section of the GLBA.[101] All individuals receiving a copy of the Order were required to sign and date an acknowledgment form indicating the receipt of the Order.

Under penalty of perjury, TaxSlayer was required to submit a compliance report and notice to the FTC.[102] The company was required to inform the FTC if it filed a bankruptcy petition or was involved in an insolvency proceeding.[103] TaxSlayer was required for 20 years to create cyber-risk assessments, accounting records, personal employee records, consumer complaints and refund requests, and any other records demonstrating full compliance with the Order. The firm was ordered to retain such records for five years after the documents were generated.[104] TaxSlayer was commanded to assign an individual to liaison between the FTC and the firm.[105] Finally, FTC stated that the Order would terminate on October 20, 2037, or twenty years from the date that the United States or the FTC filed a complaint in federal court, regardless of whether there is a settlement alleging a violation of the

---

[97] *Id.*

[98] *Id.* (See the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314).

[99] *In the Matter of TaxSlayer, LLC, supra*, note 1.

[100] Id. (First, the assessment report was due 60 days after the reporting period ended. Second, the individuals generating the assessment report must be a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA), an individual holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission. Finally, the assessment report was due to the Federal Trade Commission 10 days after the assessment report was completed).

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

Order.[106] Thus, if the FTC sues TaxSlayer sometime in the future before October 20, 2037, the 20-year compliance period starts all over again.

Lessons Learned from TaxSlayer

According to Irwin, 53 percent of successful cyber-attacks penetrate organizations without being detected, and 91 percent of all incidents do not generate an alert.[107] Although most organizations detect a cyber-attack 100 days after the attack occurs, if a firm can identify a cyber-attack within 30 days, it can save itself $1 million in expenses.[108] Irwin observed that a data breach that took less than 30 days to resolve had an average cost of $5.87 million, while the cost increased to $8.83 million for data breaches that took longer to solve.[109] FireEye noted that the majority of data breaches were discovered by a third party, typically law enforcement.[110]

Here, TaxSlayer discovered the cyber-attack approximately three weeks after the end of the attack on January 11, 2016.[111] Because of the speed at which the cyber-attack was discovered, the company probably saved about $1 million in expenses. The actual cost of the TaxSlayer cyber-attack is perhaps unknown. Before the FTC suit, the company embarked on an active campaign to alert consumers that bad actors desired to use the TaxSlayer name to achieve illicit gains.[112] In the Decision and Order, the FTC provided TaxSlayer and other companies guidance on preventing a future cyber-attack. In particular, Olcott revealed several recommended policies and procedures to help companies avert a cyber-attack, including assessing critical vendors, ensuring air-tight contracts, taking the necessary precautions, and using a continuous monitoring system.[113]

Swanagan observed that developing cyber security policies, implementing security awareness training, and installing spam filters and anti-malware software were common ways to avert a cyber-attack.[114]

---

[106] *Id.*

[107] Luke Irwin, *How Long Does It Take to Detect a Cyber Attack?*, IT GOVERNANCE, (March 14, 2019), *available at* https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack

[108] *Id.*

[109] *Id.*

[110] FireEye Staff, *Mandiant Security Effectiveness Report: Deep Dive into Cybersecurity*, FIREEYE, (n.d.), *available at* https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html

[111] *In the Matter of TaxSlayer, LLC*, *supra*, note 1.

[112] TaxSlayer Staff, *Malware Emails from TaxSlayer*, TAXSLAYER, LLC, (May 14, 2012), *available at* https://www.taxslayer.com/links/secureemails

[113] Jake Olcott, *TaxSlayer Breach: Dissecting The Latest Cyberhack*, BITSIGHT, (February 25, 2016), available at https://www.bitsight.com/blog/taxslayer-breach.

[114] Michael Swanagan, *How to Prevent Cyber Attacks*, PURPLESEC, (n.d.), *available at* https://purplesec.us/prevent-cyber-attacks/

Swanagan also recommended that companies perform periodic vulnerability assessments, routine penetration testing, security information and event management, and intrusion detection and prevention system (IDS and IPS).[115] Swanagan felt that large organizations with mature cyber security programs had dedicated red, blue, and purple teams to test the effectiveness of the firm's IT security management systems.[116] A red team is a group of people that simulate the enemy or a competitor, a blue team is a collection of individuals who defend against an attack and are typically company employees, and a purple team is a set of people who act as a red or blue team member.[117]

Conclusion

Corporations exist at the state's pleasure, but given the sectoral legal approach to privacy, corporations exist at the mercy of the state. Based on the analysis of federal sectoral privacy laws, a company should know what industries its customers are in and what federal privacy laws are associated with what industries. Given that customer exists on the company cloud, a statistical model can be created that estimates the probability of occurrence and impact of a cyber-attack on the company for a given industry. A firm should implement a stringent security framework that covers most, if not all, of the security frameworks required of its customer base. In other words, the company's security framework should encompass at least the healthcare, banking, and educational security frameworks.

There is no royal road to avoiding FTC scrutiny after a cyber-attack. *TaxSlayer* shows that once a company is attacked, it will likely be under the government's thumb for at least 20 years or more. Although the naïve response is: "Don't get hacked," there is no way to prevent a cyber-attack even if a firm is adhering to a stringent security framework. If a company experiences a cyber-attack, it is probably best to identify the malware quickly, mitigate its adverse effects, and fully cooperate with the FTC when the agency comes knocking at the corporate door. The corporation should not ask for mercy just because it was a victim of a cyber-attack. The firm should accept FTC's oversight tenure with grace and poise. If a firm behaves maturely, the sentence from the FTC may not be as draconian as meted out to TaxSlayer and other organizations. Above all, it should be remembered that the FTC is an umpire, not the enemy. By accepting responsibility for the consequences of a cyber-attack, regardless of who is at fault, the results may be only a slap on the wrist or a bump in the road. It is the best that can be hoped for.

Donald L. Buresh Biography

Donald L. Buresh earned his Ph.D. in engineering and technology management from Northcentral University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in

[115] *Id.*

[116] *Id.*

[117] *Id.*

intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity, concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée at a local fencing club. Dr. Buresh is a member of the Florida Bar.

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgments: I acknowledge the insights on risk management security frameworks that I received from Prof. Amy Apostol.

Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
AI	Artificial Intelligence
AMEX	American Express
BAA	Business Associate Agreement
BIPA	Illinois Biometric Information Privacy Act
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
COBIT	Control Objectives for Information and related Technology
CPO	Chief Privacy Officer
FedRAMP	Federal Risk and Authorization Program
FERPA	Family Educational Rights and Privacy Act
FFIEC	Federal Financial Institutions Examination council
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act

HIPAA	Health Insurance Portability and Accountability Act
IRS	Internal Revenue Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
ISACA	Information Systems Audit and Control Association
JCB	Japanese Credit Bureau
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number