International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 04 Issue 09 September 2021

DOI: 10.47191/ijsshr/v4-i9-33, Impact factor-5.586

Page No: 2512-2520

The Application of the Federal Trade Commission Privacy and Safeguards Rules to the *In the Matter Tax Slayer, LLC* Case

Donald L. Buresh, Ph.D., J.D., LL.M.
Morgan State University

ABSTRACT: This paper discusses what legally happened to TaxSlayer, LLC after a cyber break-in that occurred in 2015. The Federal Trade Commission sued the company, demanding that the organization institute robust cyber protections to ensure financial customer information security, confidentiality, and integrity. The article argues that the federal government's actions were entirely appropriate, given its constitutional mandate to regulate commerce and protect the general welfare. However, with the relentless onslaught of cybercriminal activity, the steps demanded by the federal government may prevent, but not stop, the cybercriminal tide from rising, as King Canute observed many years ago.

KEYWORDS: Covered Financial Institution, Gramm-Leach-Bliley Act, Safeguards Rule, Tax Slayer, LLC

INTRODUCTION

Many years ago, microcomputers were thought to give power to the people by allowing individuals to do things that only governments and corporations could do, namely, make calculations and process data on a massive scale. The people who worked in computing and information technology had a dream that knowledge was power, but more importantly, the ability to process data to achieve information, and thus knowledge was true power. In the intervening years, computers and their associated technologies permeated the planet, and the desire to communicate beyond mere face-to-face conversations emerged. Hence, the Internet came into being. Along with this noble goal came its counterpart, crime, as it always has in the past. Everything has its opposite, and computing was no exception to the rule.

As society gained the ability to process substantial amounts of data, cybercriminals, intent on exploiting the situation, appeared ready, willing, and able to use computing power for illicit financial gain. Governments, corporations, and even individuals that profited from this technological explosion were forced to take steps to protect themselves and their customers from the wiles of nefarious criminals that were hell-bent on exploiting this very ability. Not everyone using a computer in their daily lives took the same steps to secure the safety of their data. Laws were passed to ensure that organizations that were entrusted with protecting personal information would follow common, established standards that would avert the illegal appropriation of personal information, mainly personal financial information. In many cases, firms were reluctant to take an aggressive stance against data theft, feeling that they were too small or insignificant for criminals to bother with or because they mistrusted their government agencies. Cybercriminals, recognizing an outstanding opportunity to reap profits, understood this reluctance and exploited this prospect, many times with wild abandon.

This is one such case. TaxSlayer, LLC is a company that has greatly profited from the Internet but probably, in its zeal to grow and prosper, did not appreciate the extent of its technological vulnerabilities. When TaxSlayer was attacked by hackers stealing customer information, the Federal Trade Commission (FTC) stepped in. The federal government agency chastised and encouraged the firm to up its game, making significant technical alterations in its business model and then notifying its customers of the changes the company had done and its customers to become cyber mature.

Only time will tell if the steps ordered by the FTC will effectively prevent cybercriminals from stealing financial customer data. If the past is any indication of what will occur in the future, one thing is sure. The cybercriminals will engage in ever more clever criminal escapades, and honest organizations will consistently remain one or two steps behind them. This article deals with the efforts of the FTC and TaxSlayer to foil one instance of the onslaught of cybercrime.

The FTC Safeguards Rule Explained

In this section of the paper, the FTC Safeguard Rule and associated other notions are defined. The second subsection discusses the organizations that are subject to the FRC Safeguards Rule. The following subsection describes the compliance

requirement of the rule. Additionally, how financial information is to be secured is outlined. Finally, the essay lists proposed changes and modifications to the Safeguard Rule.

Definitions Regarding the FTC Safeguards Rule

The FTC Safeguards Rule calls for financial institutions under the FTC's jurisdiction to have policies and procedures to ensure that customer information is secure.[1] Companies that the Rule covers must confirm that their affiliates and service providers also warrant that customer information under their control is secure.[2] Sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act (GLBA) established standards for "developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[3] The purpose of the Safeguards Rule was to protect against cyber-attacks, email spoofing, phishing schemes, and similar cybersecurity risks.[4] The safeguards included administrative, physical, and technical policies and procedures and designating at least one individual, usually a separate department within an organization, responsible and accountable for all phases in developing, implementing, and testing an information security plan.[5]

Organizations That Are Subject to the FTC Safeguards Rule

Many organizations may not perceive themselves as financial institutions under the rule.[6] According to the Safeguards Rule, any business is subject to the rule, independent of its size, that is significantly engaged in delivering financial goods or services.[7] For example, currency exchanges, mortgage brokers, non-bank lenders, payday lenders, personal property and real estate appraisers, professional tax preparers, and even courier services are liable under the Safeguards Rule.[8] The rule is also applicable to credit reporting agencies and ATM operators who obtain customers' financial information from third-party financial institutions.[9] Finally, firms subject to the Rule ensure that their affiliates and partners protect financial customer information.[10]

Compliance Requirements of the FTC Safeguards Rule

According to the Safeguards Rule, entities are obliged to generate, apply, and maintain a written information security plan that explains how they will protect customer information.[11] The objectives of the program as specified in section 501(b) of the GLBA include: (1) Ensuring the security and confidentiality of customer information, (2) Protecting against known or anticipated cybersecurity threats or hazards, and (3) defending against unauthorized access or use of customer information that could result in potential harm or inconvenience to a customer.[12] The plan should be suitable to the organization's size and complexity and address the characteristics of its actions and the delicateness of the customer information that it processes. The plan should designate at least one individual to control and coordinate its information security program. The plan should also identify and assess the risks to customer information in any organization's operations.[13] According to the Safeguards Rule, a written security plan needs to evaluate the effectiveness of precautions employed for mitigating these risks and design, implement, maintain, monitor, and test the entity's security program periodically. The Safeguards Rule suggests that a covered financial institution choose service providers and vendors who possess similar information security programs. And then oversee and evaluate the information security programs of service providers and vendors, particularly when service providers and vendors alter their operations that may affect the security of customer information.[14]

---

[1] FTC Staff, *Safeguards Rule*, FEDERAL TRADE COMMISSION, (n.d.), *available at* https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule.
[2] Id.
[3] e-CFR Staff, *Part 314—Standards for Safeguarding Customer Information*, ELECTRONIC CODE OF FEDERAL REGULATIONS, (Current as of August 30, 20201), *available at* https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.
[4] Gary Kranz, *Graham-Leach-Bliley Act (GLBA)*, TECHTARGET, (Last updated June 2021), *available at* https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.
[5] Id.
[6] FTC Staff, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FEDERAL TRADE COMMISSION, (April 2006), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.
[7] Id.
[8] Id.
[9] Id.
[10] Id.
[11] e-CFR Staff, *supra*, note 3.
[12] Id.
[13] Id.
[14] Id.

The security plan may be contained in a single document or may span several documents, depending on the size and nature of the entity.[15] For example, one part of the overall plan may address the information security concerns of the information technology department, whereas another portion of the program may deal with the training or human resources department. By all means, the plan should focus on existing risks because of the unique activities or operations of the firm.[16]

How Financial Information Is to Be Secured

According to the Safeguards Rule, a covered entity must examine all areas of its operation regarding the security risks to customer information.[17] This includes employee management and training, information systems and technology, and detecting preventing breaches of its information security system.[18] The FTC suggested that an organization know the customer information in its possession and keep only the customer information it needs to engage in its business.[19] The FTC recommended that a covered financial institution manage and train its employees regarding handling customer financial information. The firm should also check references of new and existing employees that may have access to customer information and ask new and existing employees to sign a confidentiality agreement.[20]

The FTC recommended that financial institutions limit access to customer information on a need-to-know basis by requiring the use of strong passwords that employ capital and small letters, numbers, and special characters as well as employing password-activated screen savers that lock up a computer after a specified period of inactivity.[21] The FTC further suggested using encrypted files be contained on laptops, personal digital assistants (PDAs), cell phones, and other mobile devices. Employees should be trained to lock rooms and file cabinets that have sensitive customer information, avoid posting employee passwords, encrypt sensitive customer information, referring telephone calls to the appropriately designated security official; and reporting suspicious to gain customer information via social engineering was seen to be desirable activities to ensure secure customer information.[22] The FTC encouraged companies to periodically remind employees of the company's policies and procedures by advising them about the legal requirements for security while at the same time developing policies and procedures for employees that work from home.

The FTC warned covered financial institutions that there is a severe need to establish specific disciplinary measures for security violations while preventing former employees from violating the company's security policies and procedures.[23] Although it is considered an industry standard, the FTC pointed out that entities should know and keep safe customer information electronically and in hard-copy, including protection against destruction or damage from fires and floods. In other words, maintaining periodic backups of sensitive customer data and store the backups in a secure location is paramount.[24]

When appropriate, firms should avoid storing customer information on a computer that is connected to the Internet. When sending or receiving customer information, financial institutions ought to employ secure sockets layer (SSL) encryption to assure the security of the customer information.[25] A firm must request that customers via email, avoid sending an account number, social security number, etc. The FTC noted that firms need to dispose of customer information securely and in conformance with the FTC's Disposal Rule by burning, pulverizing, or shredding customer data that is no longer of economic value or after a pre-specified period. This includes computers, hard disks, flash drives, magnetic tape, etc., and printed reports.[26]

The use of current virus and spyware protection and firewalls on company computers is essential. Companies should report any security breaches, electronic or otherwise, to the appropriate corporate or law enforcement authorities and log any known security breaches in a written document that is maintained by the entity. Finally, a covered entity ought to maintain the necessary audit policies and procedures.[27]

[15] Id.
[16] Id.
[17] Id.
[18] Id.
[19] Id.
[20] Id.
[21] Id.
[22] Id.
[23] Id.
[24] Id.
[25] Id.
[26] Id.
[27] Id.

The Application of the Federal Trade Commission Privacy and Safeguards Rules to the *In the Matter Tax Slayer, LLC* Case

Proposed Change and Modifications to the Safeguards Rule

According to Nonaka et al., on March 05, 2019, the FTC asked for comments on proposed changes to the GLBA Safeguards Rule.[28] In particular, the FTC desired to expand the definition of a financial institution to include "finders," or companies that charge a fee to connect a consumer searching for a loan from a lender.[29] The FTC also proposed to amend the Privacy Rule, making technical changes resulting from amendments to GLBA that were contained in the Dodd-Frank Act and the Fixing America's Surface Transportation (FAST) Act 2015.[30] The proposed changes to the Safeguards Rules were based on the cybersecurity regulations that were recently issued by the New York Department of Financial Services (NYSDFS), along with the insurance data security model law that was published by the National Association of Insurance Commissioners (NAIC).[31]

One of the proposed changes by the FTC to the Safeguards Rule was to require companies to create and then designate an individual as the Chief Information Security Officer (CISO). Another proposed change added requirements to financial institution risk assessments. This may necessitate additional access controls on customer information systems, thereby demanding that customer information be encrypted while in transit and at rest.[32] The FTC considered requiring multi-factor authentication for individuals that accesses customer information, which may oblige customer information systems to include audit trails so that an organization can effectively detect and respond to breaches in security. The FTC wanted firms to develop procedures to dispose of ANY customer information that the entity is no longer employed.[33]

By requiring that financial institutions develop change management policies and procedures, the FTC was encouraging firms to implement policies and procedures to monitor any activities by authorized users to prevent unauthorized access, use, or tampering with customer information. Also, by demanding that entities regularly and continuously monitor vital corporate controls, systems, and procedures, they were focusing organizations on training their employees in the principles of cybersecurity, expanding company oversight of service providers and vendors, obliging financial institutions to establish incident response plans; and requiring the CISO report at least annually to the organization's board of directors regarding the entity's security program.[34]

When considering these proposed changes to the Safeguards Rule, the vote among the FTC commissioners was 3-2, where the dissenters noted that the proposed changes might be unnecessary because of the possibility of a new comprehensive data protection law.[35] Unfortunately, Congress has yet to pass comprehensive data protection legislation.[36]

The *In the Matter of TaxSlayer, LLC* Case

This section of the paper aims to discuss an example of how the FTC enforces the Safeguards Rule. The subsection will address TaxSlayer business practices and the issues before the FTC in the case. The violations of the Privacy Rule will be outlined, where it will be observed that the bulk of the case consists of the violations of the Safeguards Rule. The effects of the violations on individuals and the public will be discussed in some detail. Finally, a critique of the meaning of the case will be summarized.

TaxSlayer Business Practices

According to the FTC complaint, 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.[37] The business began more than 50 years ago when it was first only a tax preparation business. In the 1980s, the company created tax preparation software that was employed exclusively in-house, while in the 1990s, the firm developed a browser-based version of the software. In the succeeding 30 years, the organization offered a mobile tax preparation app. According to the FTC, the browser-based software service and the mobile app were the focus of the complaint.[38]

---

[28] Mike Nonaka, Libbie Canter, David Stein & Sam Adriance, *FTC Proposes to Add Detailed Cybersecurity Requirements to the GLBA Safeguards Rule*, INSIDE PRIVACY, (March 07, 2019), *available at* https://www.insideprivacy.com/financial-privacy/ftc-proposes-to-add-detailed-cybersecurity-requirements-to-the-glba-safeguards-rule/.

[29] Id.

[30] Id.

[31] Id.

[32] Id.

[33] Id.

[34] Id.

[35] Id.

[36] 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?*, SANTA CLARA UNIVERSITY HIGH TECH LAW JOURNAL, (Expected Publication Date: October 2021) (Here, it is interesting to observe that there has been administrative and legislative interest for several years in passing a comprehensive privacy law in the United States).

[37] *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.

[38] Id.

The Application of the Federal Trade Commission Privacy and Safeguards Rules to the *In the Matter Tax Slayer, LLC* Case

According to the complaint, in 2016, over 950,000 individuals filed their tax returns via TaxSlayer Online.[39] The software permitted users to create an online account by entering a user name 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 a host of other information necessary to file federal and state tax returns.[40] When all of the required information had been entered, TaxSlayer Online prepared their income tax returns, offering their customers the ability to file their returns electronically and receive any refunds by depositing the monies in their bank accounts. Customers could receive any refunds via a prepaid debit card. TaxSlayer Online charged its customers a fee for this service.[41]

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.[42] 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).[43] Because of these two reasons, TaxSlayer was subject to the GLBA Privacy Rule, and the GLBA Safeguards Rule.

Violations of the Privacy Rule

According to the FTC complaint, covered financial institutions were required by law to deliver to consumers both an initial and annual privacy notice that must be clear and conspicuous and clearly explain the firm's privacy policies and practices.[44] The privacy notice must contain specific information, including the classes of non-public personal data that TaxSlayer collected and disclosed, the types of data that third parties may receive the customer information from TaxSlayer, and the security, confidentiality, and integrity policies of the organization.[45] The complaint further opined that TaxSlayer was required to provide its privacy notice in a manner such that each consumer can reasonably expect to receive the actual notification.[46] According to the FTC complaint, TaxSlayer failed to provide its consumers a clear and conspicuous privacy notice.[47] However, the FTC did acknowledge that the privacy notices that TaxSlayer did give its customers was 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.[48] Thus, the crux of the Privacy Rule violation was that TaxSlayer should have either put its privacy notice at the beginning of its license agreement or stated its privacy policies before showing consumers the firm's licensing agreement.

Violations of the Safeguards Rule Affecting Individuals and the Public

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."[49]

In particular, 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 that they too are protecting the confidentiality, integrity, and availability of customer information, and (5) evaluate and change the information security program in light of relevant changing circumstances.[50]

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.[51] Second, TaxSlayer did not conduct a risk assessment analysis, which could

---

[39] Id.
[40] Id.
[41] Id.
[42] Id.
[43] Id.
[44] See 16 C.F.R. § 313.3(b) and 12 C.F.R. § 1016.4 and 1016.5.
[45] See 16 C.F.R. § 313.6 and 12 C.F.R. § 1016.6.
[46] See 16 C.F.R. § 313.9 and 12 C.F.R. § 1016.9.
[47] See 16 C.F.R. § 313.4 and 12 C.F.R. § 1016.4.
[48] *In the Matter of TaxSlayer, LLC*, *supra*, note 37.
[49] Id.
[50] Id.
[51] 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).

have identified internal and external risks to customer information security, confidentiality, and integrity.[52] 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.[53] TaxSlayer also did not inform its users when a customer's mailing address, password, security question, bank account routing number, or refund payment method changed.[54] TaxSlayer did not demand that customers validated their email addresses when customer accounts were created to ensure the accuracy of the customer information collected and did not employ "readily available tools" that prevented devices and IP addresses from being hacked.[55]

Furthermore, TaxSlayer was the victim of a list validation cyber-attack that began on October 10, 2015, and lasted until December 21, 2015, where on that date, the company instituted multi-factor authentication.[56] 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.[57] Finally, the FTC complaint observed that customers spend a significant amount of time resolving the consequences of cyber-attacks. Customers may be victims of identity theft, may have to obtain a new personal identification number (PIN) from the Internal Revenue Service (IRS), and may wait months for their tax refunds.[58] 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.[59]

Resolution of the TaxSlayer Case

On October 20, 2017, *In the Matter of TaxSlayer, LLC* was decided by the Federal Trade Commission.[60] The FTC restrained and enjoined TaxSlayer from violating any provision of the Privacy Rule and the Safeguards Rule. TaxSlayer was required to obtain biennial (once every two years) cyber-risk assessments and reports from a qualified, objective, and independent third-party employing generally accepted cyber-risk procedures and standards. Each assessment must contain specific administrative, physical, and technical safeguards that were instituted by TaxSlayer, which were appropriate for TaxSlayer's size, and complexity. The protections must address the nature and scope of TaxSlayer's activities and the sensitivity of guarded customer information.[61] TaxSlayer was also required to demonstrate that precautions put in place met or exceeded the defenses demanded in Section I (B) of the Order.[62] TaxSlayer was ordered to certify that its security program was sufficiently effective to reasonably assure customer information security, confidentiality, and integrity during the reporting period.[63] The FTC stated when the assessment report was done, the qualifications of the individuals creating the report, and when the report should be submitted to the FTC.[64]

Next, TaxSlayer was required to acknowledge receipt of the Order within ten days of its effective date and 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.[65] All individuals receiving a copy of the Order were required to sign and date an acknowledgment form indicating the receipt of the Order.

---

[52] *In the Matter of TaxSlayer, LLC*, *supra*, note 37.
[53] Id.
[54] Id.
[55] Id.
[56] Id.
[57] Id.
[58] Id.
[59] Id.
[60] *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.
[61] Id.
[62] Id. (See the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314).
[63] *In the Matter of TaxSlayer, LLC*, *supra*, note 60.
[64] 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).
[65] Id.

Under penalty of perjury, TaxSlayer must submit a compliance report and a compliance notice to the FTC.[66] The company was required to inform the FTC if it filed a bankruptcy petition or was involved in an insolvency proceeding.[67] 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.[68] TaxSlayer was commanded to assign an individual to liaison between the FTC and the firm.[69] Finally, FTC stated that the Oder 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 Order.[70] In other words, if TaxSlayer is sued by the FTC sometime in the future before October 20, 2037, the 20 year compliance period would start all over again.

Critique of the TaxSlayer Case

Although on its face, TaxSlayer cyber incident, and the resulting FTC complaint and resolution seem to indicate that the company was lax in its efforts to protect customer information, industry facts show that the firm was a typical cyber victim. According to Irwin, 53% of successful cyber-attacks penetrate organizations without being detected, and 91% of all incidents do not generate an alert.[71] 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.[72] 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.[73] FireEye noted that the majority of data breaches were discovered by a third party, typically law enforcement.[74]

Here, TaxSlayer discovered the cyber-attack approximately three weeks after the end of the attack on January 11, 2016.[75] 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 cyber-attacks are real and that there are bad actors out there who desire to use the TaxSlayer name in their efforts to reap illicit gains.[76] An open question is whether TaxSlayer was using state-of-the-art policies and procedures during the cyber-attack. Even so, in the Decision and Order, the FTC provided TaxSlayer and other companies, whether or not they are covered financial institutions, guidance on how to prevent 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.[77]

Swanagan observed that developing cyber security policies, implementing security awareness training, installing spam filters and anti-malware software, deploying robust firewalls, and installing an endpoint detection & response system were all common ways to avert a cyber-attack.[78] Swanagan also recommended that companies perform periodic vulnerability assessments, conduct routine penetration testing, implementing security information and event management, deploy intrusion detection and prevent software (IDS and IPS), and create a data loss prevention (DLP) program.[79] Finally, Swanagan felt that large organizations with mature cyber security programs had dedicated red, blue, and purple teams that carry out exercises to test the effectiveness of the firm's IT security management systems.[80] A red team is a group of people that simulate the enemy or a competitor, while a blue

[66] Id.
[67] Id.
[68] Id.
[69] Id.
[70] Id.
[71] 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.
[72] Id.
[73] Id.
[74] 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.
[75] *In the Matter of TaxSlayer, LLC*, *supra*, note 37.
[76] TaxSlayer Staff, *Malware Emails From TaxSlayer*, TAXSLAYER, LLC, (May 14, 2012), *available at* https://www.taxslayer.com/links/secureemails.
[77] Jake Olcott, *TaxSlayer Breach: Dissecting The Latest Cyberhack*, BITSIGHT, (February 25, 2016), available at https://www.bitsight.com/blog/taxslayer-breach.
[78] Michael Swanagan, *How to Prevent Cyber Attacks*, PURPLESEC, (n.d.), *available at* https://purplesec.us/prevent-cyber-attacks/.
[79] Id.
[80] Id.

team is a collection of individuals who defend against an attack and are typically company employees. A purple team is a set of people who can act as a read and a blue team.[81]

CONCLUSION

In some sense, TaxSlayer was a victim of circumstances where the FTC legally chided the firm for not doing enough to protect itself. The FTC Order and Decision issues may be inadequate because cybercriminals are dedicated to discovering ever more clever ways and means to attack financial institutions.[82] It is a continuous game of cat and mouse between cyber hackers and their potential victims.[83] Cybercriminals are becoming more sophisticated in circumventing even the most dynamic company efforts, at times holding corporate and consumer data hostage until a ransom is paid.[84] Organizations are also being targeted by the governments of China, Iran, and Russia.[85] Even small companies that believe that they are too small to be attacked are suffering from denial-of-service extortion attacks, where hackers are threatening to disable their ability to conduct business until the money is paid.[86] And why do hackers focus on financial institutions? Because that is where the money is!

Although TaxSlayer was sued by the FTC, the company was probably quite lucky. The cyber-attack was discovered three weeks after the end of the attack, and at the time the firm was sued, the company was likely implementing a set of policies and procedures to prevent further attacks. Even so, TaxSlayer has made significant strides in helping its customers and vendors protect themselves from future cyber-attacks.[87] If there is a lesson to be learned from *In the Matter of TaxSlayer, LLC* case, it is that no organization is immune or impervious to a cyber-attack. Constant diligence is essential, where there is no guarantee that another cyber-attack is just around the corner.

REFERENCES

1) e-CFR Staff, Part 314—Standards for Safeguarding Customer Information, ELECTRONIC CODE OF FEDERAL REGULATIONS, (Current as of August 30, 20201), available at https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.
2) Gary Kranz, Graham-Leach-Bliley Act (GLBA), TECHTARGET, (Last updated June 2021), available at https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.
3) FTC Staff, Financial Institutions and Customer Information: Complying with the Safeguards Rule, FEDERAL TRADE COMMISSION, (April 2006), available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.
4) e-CFR Staff, *supra*, note 3.
5) Mike Nonaka, Libbie Canter, David Stein & Sam Adriance, *FTC Proposes to Add Detailed Cybersecurity Requirements to the GLBA Safeguards Rule*, INSIDE PRIVACY, (March 07, 2019), *available at* https://www.insideprivacy.com/financial-privacy/ftc-proposes-to-add-detailed-cybersecurity-requirements-to-the-glba-safeguards-rule/.
6) 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?*, SANTA CLARA UNIVERSITY HIGH TECH LAW JOURNAL, (Expected Publication Date: October 2021) (Here, it is interesting to observe that there has been administrative and legislative interest for several years in passing a comprehensive privacy law in the United States).
7) *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.
8) See 16 C.F.R. § 313.3(b) and 12 C.F.R. § 1016.4 and 1016.5.
9) See 16 C.F.R. § 313.6 and 12 C.F.R. § 1016.6.
10) See 16 C.F.R. § 313.9 and 12 C.F.R. § 1016.9.
11) See 16 C.F.R. § 313.4 and 12 C.F.R. § 1016.4.
12) In the Matter of TaxSlayer, LLC, supra, note 37.

[81] Id.
[82] Ian Urbina, *Hacker Tactic: Holding Data Hostage*, THE NEW YORK TIMES, (June 14, 2014), *available at* https://www.nytimes.com/2014/06/22/sunday-review/hackers-find-new-ways-to-breach-computer-security.html.
[83] Id.
[84] Id.
[85] Id.
[86] Ud.
[87] TaxSlayer Staff, *The Importance of Tax Preparers Owning Their Role in Cybersecurity*, TAXSLAYER, LLC, (September 23, 2020), *available at* https://www.taxslayerpro.com/blog/post/tax-preparers-owning-their-role-in-cybersecurity.

13) 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).
14) In the Matter of TaxSlayer, LLC, supra, note 37.
15) *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.
16) Id. (See the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314).
17) In the Matter of TaxSlayer, LLC, supra, note 60.
18) 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).
19) 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.
20) 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.
21) In the Matter of TaxSlayer, LLC, supra, note 37.
22) TaxSlayer Staff, Malware Emails From TaxSlayer, TAXSLAYER, LLC, (May 14, 2012), available at https://www.taxslayer.com/links/secureemails.
23) Jake Olcott, TaxSlayer Breach: Dissecting The Latest Cyberhack, BITSIGHT, (February 25, 2016), available at https://www.bitsight.com/blog/taxslayer-breach.
24) Michael Swanagan, How to Prevent Cyber Attacks, PURPLESEC, (n.d.), available at https://purplesec.us/prevent-cyber-attacks/.
25) Ian Urbina, *Hacker Tactic: Holding Data Hostage*, THE NEW YORK TIMES, (June 14, 2014), *available at* https://www.nytimes.com/2014/06/22/sunday-review/hackers-find-new-ways-to-breach-computer-security.html.
26) TaxSlayer Staff, *The Importance of Tax Preparers Owning Their Role in Cybersecurity*, TAXSLAYER, LLC, (September 23, 2020), *available at* https://www.taxslayerpro.com/blog/post/tax-preparers-owning-their-role-in-cybersecurity.