YOU'VE BEEN HACKED: HOW TO BETTER INCENTIVIZE CORPORATIONS TO PROTECT CONSUMERS' DATA

Michael A. Chargo*

The number of data breaches in the U.S. has hit record highs in each of the past two years. These breaches overwhelmingly affect consumers, who have lost Social Security numbers, debit and credit card information, and birthdates. However, hackers are not targeting individual consumers; rather, they are hacking big corporations that have lax and out-of-date data security measures in place. After a data breach occurs, lawmakers and consumers alike are left wondering how and why so many preventable data breaches occur. This Article suggests that the current laws regulating data breaches are inadequate to incentivize big corporations to invest in reasonable data security practices. To remedy these shortcomings, this Article proposes that Congress adopt a uniform law regulating data security practices that holds officers and directors accountable for implementing various data protection measures.

* Michael Chargo is a 2018 graduate of Marquette University Law School, *cum laude*, and a 2015 graduate of the University of Iowa. He would like to thank Andrea Myles for her love and support while pursuing his law degree and writing this Article. He would also like to thank his family for encouraging him to attend law school. Finally, he would like to thank Apallonia Wilhelm for her valuable edits and feedback while publishing this Article.

TABLE OF CONTENTS

I. INTRODUCTION

Over the past decade, the world has seen a sharp increase in the number of data breaches involving businesses, with a record–breaking number of breaches in 2017.[1] The average cost in 2017 for a company that suffered a data breach was approximately $7.35 million.[2] Most recently, the U.S. company Equifax suffered a data breach in which hackers stole more than 143 million customers' private data.[3] Before Equifax, it was Sony that dealt with the fallout from an embarrassing data

---

[1] *2017: The Year of the Data Breach*, BLOOMBERG: PRIV. AND SEC. BLOG (Dec. 19, 2017), https://www.bna.com/2017-year-data-b73014473359; *see also* Jimmy H. Koo, *Data Breaches in U.S. Allegedly Increasing at Record Pace*, BLOOMBERG: PRIV. AND SEC. BLOG (July 24, 2017), https://www.bna.com/data-breaches-us-b73014462190 (citing *At Mid-Year, U.S. Data Breaches Increase at Record Pace*, IDENTITY THEFT RES. CTR. BLOG (July 18, 2017), https://www.idtheftcenter.org/at-mid-year-u-s-data-breaches-increase-at-record-pace). Through mid-December of 2017, the number of data breaches in the U.S. has reached a record high—1,253 publicly reported breaches. In comparison, in 2016—the previous record holder for the most data breaches—there were 1,093 breaches. *2017: The Year of the Data Breach*, *supra.*

[2] PONEMON INST., 2017 COST OF DATA BREACH STUDY: UNITED STATES 1 (2017), https://hosteddocs.ittoolbox.com/ponemon_databreach-20170825.pdf.

[3] Karen Turner, *The Equifax Hacks are a Case Study in Why We Need Better Data Breach Laws*, VOX (Sept. 14, 2017, 10:17 AM), https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security.

breach that exposed confidential employee data, as well as leaked a couple of soon-to-be released films onto the internet.[4] To add icing on the cake, the hackers released a number of emails among the executives at Sony discussing their opinions of various actors and actresses that previously worked with the studio.[5]

Although the number of data breaches is on track to reach record numbers this year,[6] consumers will likely not receive much compensation from these businesses for exposing their data. The difficulty for a consumer is proving the actual injury or damage suffered as a result of the breach.[7] In a 2014 study, 81% of consumers that were victims of a data breach did not experience any monetary harm and, when a consumer did suffer monetary harm, the average cost to the consumer was about $38.[8] However, this does not take into account the stress and time spent on the consumer's behalf,[9] which is difficult to prove in terms of monetary harm. Typically, this monetary harm does not include the long-term fallout for consumers having their private information publicly available, such as the

[4] Katelyn A. Marshall, Note, *Cyber-Security Issue: Protecting Consumers in a Cyber World—Why the Federal Trade Commission Has the Advantage*, 43 N. KY. L. REV. 105, 105–06 (2016). The hacked Sony employees' data included Social Security numbers, email addresses, and salaries. *Id.* at 105. What was likely more damaging to the company itself was the leak of two films, *The Interview* and *Annie*, available online prior to their release date. *Id.* at 105.

[5] *Id.* at 105–06. The emails also brought to light the insensitivity of the executives. Amy Kaufman, *The Embarrassing Emails that Preceded Amy Pascal's Resignation*, L.A. TIMES (Feb. 5, 2015, 1:08 PM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-amy-pascal-email-rogen-hirai-20150205-story.html. For example, Sony's Co-chairwoman at the time of the hack, Amy Pascal, had a disturbing email exchange with a big-name producer, in which the two discussed an upcoming fundraising event for President Obama. *Id.* Pascal, in discussing what she would ask President Obama, joked with the producer that she would ask the President whether he liked a number of recent movies, including *Django Unchained* and *12 Years a Slave*, starring mostly African Americans. *Id.* This email correspondence, among others, led Pascal to resign. *Id.*

[6] Koo, *supra* note 1.

[7] *See* Nicole Hong, *For Consumers, Injury is Hard to Prove in Data-Breach Cases: Judges Wrestle with Whether Hacked Firms Should Have to Compensate Exposed Customers*, WALL ST. J. (June 26, 2016, 8:06 PM), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.

[8] PONEMON INST., THE AFTERMATH OF A DATA BREACH: CONSUMER SENTIMENT 7 (April 2014).

[9] *Id.* at 6.

eventual opening of fraudulent accounts in their name or some other form of identity theft.[10]

Another significant issue that consumers face when they bring an action against a company that suffers a data breach is the constitutional standing requirement under Article III of the U.S. Constitution.[11] In many cases, the personal information that is leaked via a data breach may not have been used in a fraudulent way at the time of the lawsuit.[12] This generally is the case because hackers typically hold on to the stolen data (particularly Social Security numbers, birthdates, and names) before selling it on the black market.[13] Ultimately, the difficulty for consumers in showing the monetary harm caused by a data breach undermines their status as an injured party.[14] However, this should not relieve companies from taking reasonable measures to protect the data they obtain from consumers. After all, these companies do profit from this data.[15]

Regardless of the severity of the harm that consumers suffer from these data breaches, companies in many of these situations fail to take reasonable precautions to protect sensitive data. A 2016 report found that 63% of data breaches involve hackers exploiting weak, preset, or stolen passwords.[16] The circumstances surrounding the Equifax data breach serve as an example of a company failing to take simple steps to prevent

---

[10] *See* Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever. The Protections Offered in Their Wake Don't.*, WASH. POST (June 15, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/15/data-exposed-in-breaches-can-follow-people-forever-the-protections-offered-in-their-wake-dont/?utm_term=.5f4c356fbee8.

[11] U.S. CONST. art. III, § 2; *see also* Patricia Cave, Comment, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Court in Data Security Breach Suits*, 62 CATH. U.L. REV. 765, 768–69 (2013).

[12] Cave, *supra* note 11, at 774.

[13] Peterson, *supra* note 10 (discussing how credit and debit card numbers have a short shelf life compared to that of Social Security numbers, names, and birthdates).

[14] Cave, *supra* note 11, at 774.

[15] THE ECONOMIST INTELLIGENCE UNIT, THE BUSINESS OF DATA 7 (2016), https://eiuperspectives.economist.com/sites/default/files/images/Business%20of%20Data%20briefing%20paper%20WEB.pdf.

[16] *2016 Data Breach Investigations Report*, VERIZON ENTERPRISE SOLUTIONS 21 (2016), www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

the sensitive data of over a hundred million people from being disclosed.[17] A vulnerability in a web-application that Equifax utilized was brought to the company's attention in March of 2017.[18] Equifax failed to install the necessary updates to fix the vulnerability.[19] As a result, in May of 2017, hackers breached the web-application, stealing 143 million peoples' sensitive data.[20] Thus, Equifax had over two months to install an update that would have prevented the data breach from occurring.[21]

This Article argues that the current legal framework for data security suffers numerous problems that undermine its effectiveness at ensuring that companies protect sensitive consumer data. Those problems include gaps in the law due to industry specific federal statutes, a compliance nightmare for large corporations having to comply with multiple states' potentially different laws, and a reactive rather than proactive approach to improving data security practices. Part II discusses the current legal framework for data privacy in the U.S. Part III then reviews a number of the high-profile data breaches over the past five years as proof that the current legal framework is ineffective at incentivizing companies to implement reasonable data security measures. Finally, Part IV proposes that Congress create a uniform federal data privacy statute that creates a two-tracked approach to regulating data security.

II. THE CURRENT DATA SECURITY AND PRIVACY LEGAL LANDSCAPE

This section will separate the current laws and rules governing data privacy into three categories, analyzing the categories from most to least impactful in terms of regulating data security. The first category, discussed in Section A, focuses on the rules created by federal regulatory agencies to monitor data security practices. The second category, discussed in Section B, views the federal laws that regulate data security. The final category, discussed in Section C, notes the protections afforded by state law.

---

[17] *See* Lely Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017, 1:27 PM), https://www.wired.com/story/equifax-breach-no-excuse/.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

Ultimately, these three categories show that the current legal landscape in the area of data security fails to motivate companies to adopt reasonable data security practices.

A. The Most Significant Source of Data Security Regulation: Federal Regulatory Agencies

The Federal Trade Commission (FTC) is perhaps the most established regulatory agency monitoring data security at this time. The FTC derives its authority for governing data security from Section 5(a) of the Federal Trade Commission Act (FTC Act).[22] Generally, Section 5(a)(2) of the FTC Act states, "The [FTC] is hereby empowered and directed to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[23] The statute defines unfair and deceptive practices as those acts that "cause or are likely to cause reasonably foreseeable injury within the United States. . . ."[24] Since 2002, the FTC has brought more than 60 cases against companies for unfair or deceptive practices that unreasonably risked exposing consumers' data.[25] However, recently some of these companies have challenged the FTC's authority to regulate data security practices under Section 5.[26]

In *FTC v. Wyndham Worldwide Corp.*,[27] Wyndham Worldwide Corporation (Wyndham) suffered three data breaches over a two-year

---

[22] Crystal N. Skelton, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 No. 1 Competition: J. ANTI., UCL & PRIVACY SEC. ST. B. CAL. 302, 303 (2016).

[23] 15 U.S.C. § 45(a)(2) (2016).

[24] *See Id.* § 45(a)(4)(A). Notably, the statute does not enumerate specific kinds of business practices that constitute unfair and deceptive acts. *See generally id.* Marshall, *supra* note 4, at 112 n.58.

[25] FTC, PRIVACY & DATA SECURITY: UPDATE: 2016, at 4 (2016), https://www.ftc.gov/reports/privacy-data-security-update-2016.

[26] Skelton, *supra* note 22, at 306. This Article will focus solely on the Wyndham case, although another company, LabMD, challenged the FTC's authority as well to regulate data security. *In re* LabMD, Inc., No. 9357, 1, 5 (F.T.C. July 29, 2016). In this case, the Commission reversed the administrative law judge (ALJ), holding that the ALJ applied the wrong legal standard for unfairness. *Id.* The Commission concluded that LabMD's cybersecurity practices constituted an unfair practice within the meaning of Section 5(a) of the FTC Act. *Id.*

[27] 799 F.3d 236 (3d Cir. 2015).

period.[28] The hackers stole hundreds of thousands of customers' personal and financial data, resulting in over $10.6 million dollars in fraudulent charges.[29] The FTC filed a lawsuit against Wyndham in federal district court alleging that Wyndham engaged in unfair and deceptive data security practices leading to the data breach.[30] Wyndham filed a motion to dismiss the FTC's suit, which was denied by the district court.[31] However, the district court certified its ruling for interlocutory appeal on two issues.[32] The first issue was whether the FTC had the authority to regulate cybersecurity under the unfairness prong of Section 5(a) of the FTC Act.[33] The second issue was whether Wyndham received fair notice that its data protection practices could violate the unfairness prong.[34] On the first issue, the Third Circuit held that the FTC has authority under the unfairness prong to regulate cybersecurity.[35] The Court on the second issue held that "Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices were required" under Section 5(a).[36] Rather, Wyndham simply had to know that its data security practices could be governed by the statute.[37] Ultimately,

---

[28] *Id.*

[29] *Id.*

[30] *Id.* Specifically, the FTC listed seven practices that Wyndham engaged in that were the basis for the unfair and deceptive practices action: (1) the company allowed its hotels to store consumer payment data in an unencrypted format, making the data clearly readable; (2) Wyndham permitted the use of weak passwords for accessing the company's property management system; (3) there was a failure to use commonplace data security measures like firewalls; (4) the company failed to implement adequate data security policies and procedures leading to out-of-date software; (5) Wyndham did not limit the access of its third-party vendors so as to prevent them from accessing the company's network and servers; (6) there was not an appropriate system in place for detecting and preventing unauthorized access to the company's networks and servers; and (7) Wyndham did not follow any sort of procedures for responding to the first hack, allowing the hackers to use a similar exploitation for the second and third hacks. *Id.* at 240–41; Skelton, *supra* note 22, at 307 (referencing the outcome of this lawsuit).

[31] Wyndham, 799 F.3d at 242; Skelton, *supra* note 22, at 307.

[32] Skelton, *supra* note 22, at 307.

[33] *Id*; Wyndham, 799 F. 3d at 242.

[34] Skelton, *supra* note 22, at 307; Wyndham, 799 F.3d at 249.

[35] Wyndham, 799 F.3d at 247–49.

[36] *Id.* at 255–58.

[37] *Id.*

this case clarifies the authority the FTC has to regulate unfair and deceptive data security practices under Section 5(a) of the FTC Act.[38]

Since the FTC has the power to regulate unfair and deceptive data security practices, the focus now shifts to its methodology for curbing such practices. Broadly speaking, the FTC divides its focus into deception claims and unfairness claims when regulating data security practices.[39] For deception claims, the FTC is focused on whether a business misrepresented its privacy and security practices, or its controls for protecting consumer data related to one of its products.[40] Alternatively, for an unfairness claim, the FTC is focused on businesses that fail to implement or maintain reasonably adequate data protection mechanisms for protecting consumers' personal information in a way that causes or is likely to cause significant injury to the consumer.[41] The FTC adds a qualifier by stating that the injury to the consumer cannot be outweighed by the benefits to the consumer, nor can the injury be reasonably avoidable by the consumer.[42]

On the day that the FTC reached its 50th data security settlement, it commented on its overall method for regulating unfair and deceptive data security practices, stating:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[43]

---

[38] Marshall, *supra* note 4, at 120.

[39] Skelton, *supra* note 22, at 304.

[40] *Id*; *see* FTC POLICY STATEMENT ON DECEPTION 2 (October 14, 1983) (discussing standards of misrepresentation).

[41] Skelton, *supra* note 22, at 304; *see* FTC POLICY STATEMENT ON UNFAIRNESS (December 17, 1980) (discussing standards of consumer injury, violations of public policy, and unethical or unscrupulous conduct).

[42] Skelton, *supra* note 22, at 304; *see* FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 41.

[43] FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (2014).

The FTC's methodology in regulating data security practices appears to be a sliding-scale approach. Besides these insights, the FTC published a guide providing businesses with five key principles to data protection.[44] Those five key principles are: (1) "[k]now what personal information you have in your files on your computers," (2) "[k]eep only what you need for your business," (3) "[p]rotect the information that you keep," (4) "[p]roperly dispose of what you no longer need," and (5) "[c]reate a plan for responding to security incidents."[45] These factors, and the FTC's approach more broadly, all focus on companies implementing reasonable data security practices.

As discussed in Part III, a number of large companies have failed to follow these principles, which ultimately has led to massive data breaches.[46] This calls the effectiveness of the FTC's current approach into question. Since the FTC brought its first action in 2002, the FTC has brought over 60 actions against businesses for unfair and deceptive data security practices.[47] Nevertheless, the overall number of data breaches has increased over this period of time.[48] One could argue that the increase in data breaches is a natural result of the increased amount of data that today's current society creates and stores electronically on servers.[49] However, such an argument fails to focus on the unreasonable data security practices of many companies that lead to these breaches. If the amount of electronic data continues to increase in our society,[50] then we need to incentivize companies to do a better job at protecting that data. Thus, this shows that the FTC's reasonableness approach, currently and in the future, will fail to adequately incentivize companies to take reasonable data security measures that will reduce the number of breaches disclosing consumers' personal data.

---

[44] FTC, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 1 (2016) [hereinafter PPI: A Guide for Business].

[45] *Id.* at 2–30.

[46] *See infra* Part III.

[47] FTC, PRIVACY & DATA SECURITY: UPDATE: 2016, at 4 (2016).

[48] Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (July 27, 2017), https://digitalguardian.com/blog/history-data-breaches (noting that the number of data breaches in 2005 was 157 compared to 783 in 2014).

[49] *Id.*

[50] *Id.*

The other regulatory agency that has recently started regulating data security is the Consumer Financial Protection Bureau (CFPB). Specifically, the CFPB recently began regulating financial institutions that engage in unfair and deceptive cybersecurity practices, bringing its first ever enforcement action in March of 2016.[51] Congress gave the CFPB the power to regulate unfair and deceptive practices in 2010 with the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act.[52] The grant of authority given to the CFPB mirrors much of the same language that serves as the basis for the FTC's authority under Section 5(a) of the FTC Act.[53] The main difference between the authority granted to the FTC and the CFPB is that the CFPB is limited to bringing actions against financial institutions or businesses that are involved in the financial industry.[54] Because the CFPB's first and only enforcement action related to cybersecurity occurred in March of 2016,[55] it is still too early to determine the regulatory impact the CFPB may potentially have in bringing enforcement actions against financial companies that have unfair and deceptive data security practices. If the FTC's approach is effective in combating data breaches, then one would think that the CFPB would have similar success in regulating the financial industry.

However, the CFPB's authority to regulate data security practices is limited to the financial industry,[56] which limits its overall effectiveness. In 2016, only 9% of the data breaches involving the financial industry disclosed personal information, compared to 27% in the retail industry and 45% in the information industry (which includes social media sites and cloud storage servers).[57] This exemplifies why the CFPB's regulation

---

[51] *CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices*, CFPB (Mar. 2, 2016), https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[52] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 2005 (codified at 12 U.S.C. § 5531 (2010)).

[53] *Compare* 15 U.S.C. § 45(a)(2) (2016) *with* 12 U.S.C. § 5531(a).

[54] 12 U.S.C. § 5481(6) (2010).

[55] *See* Evan Weinberger, *Equifax Data Breach Highlights Regulatory Shortfall*, LAW 360 (Sept. 8, 2017, 8:45 PM), https://www.law360.com/articles/962025/equifax-data-breach-highlights-regulatory-shortfall.

[56] *Compare* 15 U.S.C. § 45(a)(2) *with* 12 U.S.C. § 5531(a).

[57] *2017 Data Breach Investigations Report*, VERIZON ENTERPRISE SOLUTIONS 19, 24, 30 (2017),

of data security practices in the financial industry would have a limited impact in protecting consumers more generally. Finally, there is currently uncertainty surrounding the fate of the agency, as its constitutionality has recently been called into question.[58]

B. A Potpourri of Federal Law

The current federal legislation directly governing data security in the United States is a hodgepodge of industry-specific statutes.[59] Currently, there is no uniform federal statute governing data security and privacy.[60] The lack of a uniform federal data security law creates a number of gaps in which various industries, outside of the financial and healthcare sectors, face little to no data security regulation outside of breach notification laws.[61] In addition, most of the industry-specific laws center around businesses in those industries disclosing their data protection practices and using care when handling sensitive consumer data.[62] As discussed previously, the FTC Act authorizes the FTC to regulate unfair and deceptive trade practices.[63] The remainder of this section will examine some of the other well-known federal statutes providing data protection.

The Financial Services Modernization Act (also known as the Gramm-Leach-Bliley Act) requires the FTC, among other regulatory agencies that monitor financial institutions, to enforce its privacy provisions.[64] To fulfill its requirements, the FTC created the Privacy of

---

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf.

[58] Renae Merle, *Federal Judge Rules that Consumer Protection Bureau is Unconstitutional*, CHICAGO TRIBUNE (June 21, 2018, 5:05 PM), http://www.chicagotribune.com/business/ct-biz-judge-rules-cfpb-unconstitutional-20180621-story.html.

[59] *See, e.g.* Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2012); Financial Services Modernization Act (Gramm-Leach-Bliley Act), 15 U.S.C. §§ 6801–27 (2012); Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1301 (2012); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

[60] Skelton, *supra* note 22, at 305.

[61] Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 52–54 (2015).

[62] Marshall, *supra* note 4, at 108.

[63] *See supra* text accompanying notes 22–24.

[64] 15 U.S.C. § 6822 (2012).

Consumer Financial Information Rule (Privacy Rule).[65] This Rule covers two categories of businesses: (1) financial institutions and (2) businesses that receive "nonpublic personal information" from financial institutions of which they are not affiliated.[66] "Nonpublic personal information" (NPI) is defined as any personally identifiable financial information that a financial institution obtains about an individual in the course of providing a financial product or service, except if the information is generally publicly available.[67] Information that is publicly available is described as information that is lawfully available to the public, and the individual can direct that the information not be made public but has not done so.[68] Ultimately, the Privacy Rule only provides requirements and guidance for what is required of businesses in terms of disclosing to consumers their company's privacy policies and practices.[69]

However, the FTC created a Safeguards Rule to regulate business's protection of NPI.[70] The Safeguards Rule requires, among other things, that businesses adopt a written security plan that includes: (1) designating one or more employees to manage the security program,[71] (2) methods for identifying and assessing the risks to customer information in each facet of the company's business, as well as analyzing the effectiveness of the current safeguards in place,[72] (3) policies for designing, implementing, and

---

65 *See* 16 C.F.R. § 313.1 (2012).

66 FTC, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 2 (2002).

67 *Id.* at 4. The FTC elaborates on types of information that are considered NPI by providing three areas in which information obtained by a business will constitute NPI: (1) any information that a person provides a business for the purpose of receiving a financial service or product, including name, address, income, Social Security number, etc.; (2) any information that an individual provides a business in the course of a transaction involving the business's financial product or service, including credit or debit card information, payment history, the fact that the individual is a consumer, etc.; and (3) any information that a business obtains about an individual in connection with providing a financial service or product, including court records or consumer reports. *Id.*

68 *Id.* at 5.

69 *Id.* at 6–13.

70 FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. § 314.1(a) (2012).

71 *Id.* § 314.4(a).

72 *Id.* § 314.4(b)(1)–(3).

regularly testing the security program,[73] (4) standards for partnering with service providers that are capable of maintaining appropriate safeguards,[74] and (5) internal requirements for evaluating and revising the company's security program based on the testing and monitoring requirement in (3).[75] Overall, the Safeguards Rule appears comprehensive in its requirements. But, as a practical matter, in many cases the FTC will only learn of violations of the Safeguards Rule once a data breach has already occurred. Since 2010, the FTC has brought six actions against businesses for violating the Safeguards Rule under the Gramm-Leach-Bliley Act.[76] Four out of the five actions were in response to a business that already suffered a data breach.[77] Therefore, the enforcement of the Safeguards Rule is reactive rather than proactive, meaning a hacker has already obtained a consumer's NPI by the time the FTC brings an enforcement action. In addition, the Safeguards Rule only applies to financial institutions or businesses involved in the financial industry, which limits its applicability to a small subset of businesses.

The other well-known federal statute governing data security is the Health Insurance Portability and Accountability Act of 1996 (also referred to as HIPAA).[78] Congress tasked the U.S. Department of Health and Human Services (HHS) with developing and regulating privacy and security of health information.[79] To meet these statutory obligations, the

---

[73] *Id.* § 314.4(c).

[74] *Id.* § 314.4(d)(1)–(2).

[75] *Id.* § 314.4(e).

[76] *See Cases and Proceedings: Advanced Search: Consumer Protection Topics: Gramm-Leach-Bliley Act*, FTC: ENFORCEMENT, https://www.ftc.gov/enforcement/cases-proceedings/advanced-search (select "Gramm-Leach-Bliley Act" from the "Consumer Protection Topics" dropdown menu) (last visited Mar. 22nd, 2018).

[77] *See* Complaint at 4–5, para. 15–18, *In re* Taxslayer, LLC, (No. C-4626) (F.T.C. Oct. 20, 2017); Compliant at 2–4, para. 6–12, *In re* ACRAnet, Inc. (No. C-4331) (F.T.C. Aug. 17, 2011); Complaint at 2–4, para. 8–14, *In re* Fajilan & Assocs., (No. C-4332) (F.T.C. Aug. 17, 2011); Complaint at 2–4, para. 8–14, *In re* SettlementOne Credit Corp., (No. C-4330) (F.T.C. Aug. 17, 2011). *But see* Complaint at 5–9, para. 15–19, 27–29, United States v. PLS Financial Services, Inc., (No. 1:12-cv-08334) (N.D. Ill. Oct. 17, 2012) (noting that the defendants misrepresented data security policies to consumers).

[78] Marshall, *supra* note 4, at 108.

[79] Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d-2 (2009).

HHS developed two rules: (1) the "Standards for Privacy of Individually Identifiable Health Information" and (2) the "Security Standards for the Protection of Electronic Protected Health Information."[80] The distinction between these two rules is that the first rule is geared towards regulating which covered entities may have access to protected health information (PHI), while the second rule establishes standards for protecting electronic PHI (EPHI) from unauthorized access.[81] Thus, the focus here will be on the Security Standards for the Protection of EPHI as it is more pertinent to the topic of data breaches.

In general, the security standards are divided into three categories.[82] First, there are administrative safeguards, which establish eight standards for companies to follow in relation to managing and training requirements for EPHI protection.[83] Second, there are physical safeguards that create four standards that mostly relate to actual access and protection of the electronic systems and equipment that store EPHI.[84] Finally, there are technical safeguards that generally institute five standards dealing with authentication controls and minimum hardware and software requirements for protecting EPHI.[85] However, these standards only apply to "covered entities," which are generally health care providers, health plans, and health care clearing houses.[86] This makes the scope of these data security protections rather narrow.

Outside the financial and health sectors, there is little to no federal law protecting consumers' sensitive data.[87] In addition, most of the federal laws governing data breaches involve the kinds of disclosures and notices

---

[80] *Summary of the HIPAA Security Rule*, U.S. DEP'T OF HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 16th, 2017).

[81] U.S. Dep't of Health & Human Servs., *Security 101 for Covered Entities*, HIPAA SEC. SERIES 4 (MAR. 2007).

[82] *Id.* at 8.

[83] 45 C.F.R. § 164.308(a)(1)–(8).

[84] *Id.* § 164.310(a)–(d).

[85] *Id.* § 164.312(a)–(e).

[86] U.S. Dep't of Health & Human Servs., *supra* note 81, at 2–3.

[87] Marshall, *supra* note 4, at 108; Skelton, *supra* note 22, at 306.

a business must make to a consumer once a breach has already occurred.[88] Some have suggested that this lack of a uniform federal data security law has fostered an environment where businesses have no incentive to maintain high levels of security and protection for their data.[89] However, as the number of data breaches continue to rise, experts have begun to call on Congress to adopt a uniform federal statute governing data privacy and security.[90] A potential framework for data protection and security is discussed Part IV.

C. The Scope of State Laws

Due to the gaps that the industry-specific federal laws have created, state laws have been left to fill in the holes.[91] Most of the state legislation pertaining to data breaches surrounds the notification requirements for businesses that have already suffered a breach.[92] As of March 2018, all fifty states and the District of Columbia have adopted some form of legislation requiring businesses to notify individuals of security breaches where personally identifiable information is exposed.[93] However, the immense number of state statutes creates a compliance headache for many large businesses, as those businesses could potentially have to comply with fifty states' differing data breach notification laws.[94] Moreover, some of these data breach laws may conflict in terms of what triggers the duty to notify a consumer.[95] For example, Connecticut requires a company to notify a consumer if there has been unauthorized access to electronic files containing personal data.[96] Alternatively,

---

[88] Laura Hautala, *Equifax Hack May Shake Up US Consumer Data Laws: Federal Lawmakers are Pushing to Give You More Control Over Your Data, After Hackers Stole Information from 145 million Americans*, CNET (Oct. 20, 2017, 9:00 AM), https://www.cnet.com/news/equifax-hack-may-shake-up-consumer-data-laws/.

[89] Marshall, *supra* note 4, at 106.

[90] *Id.* at 106–09; Weinberger, *supra* note 55.

[91] Tschider, *supra* note 61, at 52; Skelton, *supra* note 22, at 305–06.

[92] Skelton, *supra* note 22, at 305–06.

[93] Security Breach Notification Laws, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1 (last visited Sept. 1, 2018).

[94] Tschider, *supra* note 61, at 64.

[95] *Id.*

[96] CONN. GEN. STAT. § 36a-701b(b)(1) (2015).

Wisconsin only requires a business to notify a consumer if the unauthorized acquisition of the personal information creates a material risk of identity theft or fraud for the affected consumer.[97] Although businesses could try to comply with the most restrictive state's data breach notification laws, conflicting state laws still create a compliance headache for large businesses because they would constantly have to monitor fifty different states' laws to ensure it stays abreast of any changes.

Additionally, fifteen states have adopted some form of law requiring businesses to maintain reasonable data security practices.[98] Thus, although some states have enacted data security requirements that

---

[97] WIS. STAT. § 134.98(2)(cm)(1) (2015–2016).

[98] Data Security Laws—Private Sector, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx (last visited Sept. 1, 2018). The states that do require some sort of reasonable data security practice include: (1) ARK. CODE ANN. § 4-110-104(b) (2017) (requiring businesses to "implement and maintain reasonable security procedures and practices"); (2) CAL. CIV. CODE § 1798.81.5(b) (2016) (requiring businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information"); (3) CONN. GEN. STAT. § 42-471(a) (2017) (requiring business to "safeguard the data, computer files and documents" containing personal information); (4) FLA. STAT. § 501.171(2) (2014) (requiring businesses to "take reasonable measures to protect and secure data in electronic form containing personal information"); (5) IND. CODE § 24-4.9-3-3.5(a) (2017) (requiring businesses to "maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information"); (6) KAN. STAT. ANN. § 50-6, 139(b)(1) (2017) (requiring businesses to "[i]mplement and maintain reasonable procedures and practices appropriate to the nature of the information"); (7) MD. CODE ANN. § 14-3503 (West 2017) (requiring businesses to "implement and maintain reasonable security procedures and practices"); (8) MASS. GEN. LAWS ch. 93H, § 2 (2017) (authorizing its department of consumer affairs and business regulation to adopt regulations that "safeguard the personal information of residents"); (9) MINN. STAT. § 325M.05 (2017) (governing the conduct of internet service providers stating that they "shall take reasonable steps to maintain the security and privacy of a consumer's" sensitive data); (10) NEV. REV. STAT. § 603A.210 (2017) (requiring businesses to "implement and maintain reasonable security measures to protect those records from unauthorized access"); (11) N.M. STAT. ANN. § 57-12C-4 (2017) (requiring businesses to "implement and maintain reasonable security procedures and practices"); (12) OR. REV. STAT. § 646A.622 (2017) (adopting a framework similar to HIPAA requiring businesses to implement a security program that includes three categories of safeguards: administrative safeguards, technical safeguards, and physical safeguards); (13) 11 R.I. GEN. LAWS ANN. § 11-49.3-2 (West 2017) (requiring businesses to "implement and maintain a risk-based information security program that contains reasonable security procedures and practices"); (14) TEX. BUS. & COM. CODE ANN. § 521.052 (West 2017) (requiring businesses to "implement and maintain reasonable procedures . . . to protect from unlawful use or disclosure" of sensitive data); and (15) UTAH CODE ANN. § 13-44-201 (West 2017) (requiring businesses to "implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information").

demand more from businesses than notifying consumers of a breach, more than half of states only have data breach notification statutes.[99] Data breach notification laws are inadequate as they are reactive in nature: a data breach has already occurred by the time that a data breach notification law comes into play. Once a data breach occurs, hackers could have already stolen a consumer's personal information. Therefore, data breach laws need to require companies to protect the sensitive data up front so as to prevent a breach from happening in the first place. As alluded to above, the difficulty with a large number of states adopting more stringent data security laws is the compliance difficulties that arise from a lack of a uniform standard. This suggests that a uniform law is needed to help mitigate the compliance difficulties that would arise from forty-eight states each having their own data security protection laws.

Another area of state law that has largely been ineffective in curbing the amount of data breaches is the fiduciary duty requirements for boards of directors and corporate officers.[100] To start, the board of directors and officers only owe fiduciary duties to the corporation and its shareholders, not to the consumers that are harmed by the data breaches.[101] Further, two high-profile derivative suits stemming from data breaches over the past five years have failed.[102]

In the first of the lawsuits, a stockholder of Wyndham Worldwide Corporation sent a letter to the board of directors demanding the board investigate and remedy the harm caused by the data breaches.[103] After the board decided not to file a lawsuit based on the breaches, the plaintiff stockholder filed a derivative suit against Wyndham and a number of its corporate officers, alleging that the company failed to implement and

---

[99] *See* Data Security Laws—Private Sector, *supra* note 98.

[100] Joseph B Crace, Jr. & Virginia M. Yetter, *When Does Data Breach Liability Extend to the Boardroom?*, LAW 360 (Apr. 3, 2017, 12:43 PM), https://www.law360.com/articles/907786.

[101] William M. Lafferty et al., *A Brief Introduction to the Fiduciary Duties of Directors Under Delaware Law*, 116 PENN. ST. L. REV. 837, 841 (2012); Jonathan R. Macey, *Fiduciary Duties as Residual Claims: Obligations to Nonshareholder Constituencies from a Theory of the Firm Perspective*, 84 CORNELL L. REV. 1266, 1273 (1999).

[102] Crace, Jr. & Yetter, *supra* note 100.

[103] Palkon v. Holmes, No. 2:14–CV–01234 (SRC), 2014 WL 5341880, at *2 (D.N.J. Oct. 20, 2014).

maintain proper data security practices.[104] The court dismissed the suit holding that the plaintiff failed to plead facts, with particularity, that establish that the board acted either in bad faith or based on an unreasonable investigation.[105] Therefore, the board's decision not to file a lawsuit based on the breaches received the protection of the "business judgment rule."[106]

The second lawsuit involved a shareholder of The Home Depot suing twelve current and former corporate officers and directors of the company.[107] The shareholders alleged that the officers and directors breached their duty of loyalty by not implementing proper internal controls to oversee the risks that the company faced due to a potential data breach.[108] Moreover, the shareholders supported this allegation of a breach of loyalty based on the fact that the board of directors disbanded the committee that was tasked with overseeing the risks that could stem from a data breach.[109] Ultimately, the court granted the defendants' motion to dismiss, holding that the shareholders failed to plead facts, with particularity, that the board consciously failed to act in the face of a known duty to act.[110] The court found that the shareholders admitted that the board acted before the breach occurred by approving a new data security plan that would have remedied many of the vulnerabilities Home Depot currently faced.[111] The plan was simply not fully implemented at the time the breach occurred.[112]

Despite these two recent examples of derivative suits arising from data breaches failing, there are currently a number of other derivative suits

---

104 *Id.*

105 *Id.* at *3.

106 *Id.*

107 *In re* The Home Depot, Inc. Shareholder Derivative Litigation, 223 F. Supp. 3d 1317, 1320–21 (N.D. Ga. 2016), *appeal docketed, sub nom.* Bennek v. Ackerman, No. 16-17742 (11th Cir. Dec. 28, 2016).

108 *Id.* at 1321.

109 *Id.*

110 *Id.* at 1327, 1331–32.

111 *Id.* at 1327.

112 *Id.*

still unresolved, including lawsuits involving Yahoo! and Wendy's.[113] Thus, there is a possibility that such lawsuits could start succeeding if plaintiffs begin including more facts in the pleading stage.[114] Nevertheless, derivative suits do not provide a remedy for the consumers whose sensitive data was obtained during these data breaches. Rather, these derivative suits are used by shareholders in an attempt to recover the amounts these companies paid out to consumers and others as a result of the data breach.[115] This, along with the many different state laws governing data breach notification, shows that state law is inadequate for forcing businesses to adopt better data security practices.

III. RECENT HIGH-PROFILE DATA BREACHES

As discussed previously, the FTC is arguably in the best position to regulate and enforce data security laws.[116] The FTC's approach to regulating data privacy and security is one of reasonableness.[117] After the FTC's 50th data security settlement, the FTC stated:

> The Commission will continue its efforts to educate businesses on reasonable data security practices to help them prevent future breaches from occurring. The commission's body of fifty data security settlements reflects its commitment to ensure that companies employ reasonable measures to safeguard consumer data. As the commission moves forward, it will continue to hold companies accountable for practices that violate the law by falling short of this standard.[118]

---

[113] Crace, Jr. & Yetter, *supra* note 100.

[114] *Id.*

[115] *See, e.g., In re* The Home Depot, Inc., 223 F. Supp. 3d at 1320–23; Palkon, 2014 WL 5341880, at *1–2.

[116] *See* Marshall, *supra* note 4, at 123–27; *see* Skelton, *supra* note 22, at 306.

[117] *See supra* text accompanying notes 43–45.

[118] FTC, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 2 (2014).

To assess the effectiveness of the FTC's approach, this section will review some of the most significant data breaches that have occurred over the past five years to evaluate whether these companies took reasonable measures, such as the five principles articulated by the FTC,[119] to protect sensitive data. The following examples show large corporations, with ample resources, that failed to take basic, reasonable measures to protect sensitive consumer data. These companies' failures led to some of the largest data breaches in history.[120]

A. Target

In the fall of 2013, hackers accessed Target's computer network and stole financial and personal information from more than 110 million customers.[121] On December 19, 2013, Target publicly announced that 40 million credit and debit card accounts were compromised in the breach.[122] Less than a month later, on January 10, 2014, Target indicated that roughly 70 million customers had non-financial data stolen during the same breach.[123] The stolen data was then sold on various black market forums, with many banks not having enough time to identify and cancel stolen cards before fraudulent purchases were made.[124]

Ultimately, an analysis of the data breach showed that Target failed in four ways to either stop the hackers or prevent the data breach from occurring.[125] First, Target provided a third-party vendor with network access.[126] The vendor did not follow the commonly accepted industry standards for protecting information, which allowed the hackers to enter Target's network.[127] Second, Target ignored numerous automated

---

[119] *See generally* PPI: A Guide for Business, *supra* note 44, 1–30.

[120] Elizabeth Weise, *Equifax Breach: Is it the Biggest Data Breach?*, USA TODAY (Sept. 7, 2017), https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/.

[121] Majority Staff Rep't for Chairman Rockefeller, S. COMM. ON COMMERCE, SCI., & TRANSP., A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH, i (2014).

[122] *Id.* at 1.

[123] *Id.* at 2.

[124] *Id.* at 1.

[125] *Id.* at i.

[126] *Id.*

[127] *Id.*

warnings from its data protection software, including warning messages that indicated that attackers were installing malware on Target's network.[128] Third, there was evidence based on the way the hackers moved within Target's network that the attackers started in a less sensitive area of the network before moving to the high sensitive areas storing consumer data, which potentially means that Target did not effectively protect its most sensitive data networks.[129] Fourth, Target failed to respond to its own warning systems indicating the "escape routes" the hackers planned on exploiting to steal the data from the network.[130]

Overall, Target was held accountable for its unreasonable data security practices. Target settled a class-action with the consumers harmed by the data breach for $10 million.[131] Additionally, Target agreed to pay forty-seven states and the District of Columbia $18.5 million to settle the claims that could have been brought under these states' various consumer protection acts, personal information protection acts, and security breach notification acts.[132] Finally, Target settled class-action claims with a number of U.S. financial institutions, including Visa and MasterCard, for more than $100 million.[133] Nonetheless, these settlements were reactive, occurring after hackers already stole the consumer data and sold it on the black market. Instead, the current laws regulating data security practices need to require companies to be proactive in taking

---

128 *Id.*

129 *Id.*

130 *Id.*

131 George Stahl, *Target to Pay $10 Million in Class Action Over Data Breach*, WALL ST. J. (March 19, 2015, 8:38 AM), https://www.wsj.com/articles/target-to-pay-10-million-in-class-action-over-data-breach-1426768681.

132 Sruthi Ramakrishnan & Nandita Bose, *Target in $18.5 Million Multi-State Settlement Over Data Breach*, REUTERS (May 23, 2017, 11:39 AM), https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-state-settlement-over-data-breach-idUSKBN18J2GH; *see also* BUREAU OF INTERNET & TECH., N.Y. ATT'Y GEN., ASSURANCE NO. 17-094, IN RE INVESTIGATION BY ERIC T. SCHNEIDERMAN, ATT'Y GEN. OF THE STATE OF N.Y., OF TARGET CORP. 1–12 (2017), https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf (notably the settlement did not involve any federal agency).

133 Ezequiel Minaya, *Target Reaches Another Data Breach Settlement: The Retailer Agreed to Reimburse MasterCard and Other Companies $39 Million related to the 2013 Breach*, WALL ST. J. (Dec. 2, 2015, 6:10 PM), https://www.wsj.com/articles/target-reaches-another-data-breach-settlement-1449085790.

reasonable steps to prevent these data breaches from occurring in the first place.

B. Home Depot

In September of 2014, Home Depot informed consumers that its payment card systems were hacked, with 56 million payment cards stolen during the breach.[134] To make matters worse, the method in which the hackers accessed Home Depot's network was the same way the hackers infiltrated Target's network.[135] Ultimately, this breach was larger than the one that Target suffered, even though the Target breach happened almost a year earlier.[136] Home Depot, along with other companies, should have learned from the Target data breach to protect their payment card systems.[137] This highlights the fact that monetary penalties that are enforced either by federal regulatory agencies, like the FTC, or by states do not motivate companies to be proactive in taking reasonable data security measures. Thus far, Home Depot has reached settlements agreeing to pay more than $27 million to financial institutions[138] and $19.5 million to the consumers harmed.[139] Currently, there are a number of states investigating the Home Depot data breach.[140] However, the FTC has still not taken any action against the company, even after two U.S. Senators called on the FTC to investigate the data breach.[141] In terms of

---

134 Brett Hawkins, *Case Study: The Home Depot Data Breach*, SANS INSTITUTE 2, 4 (Jan. 2015), https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367.

135 *Id.* at 7.

136 *Id.* at 3–4.

137 *Id.* at 4.

138 Dena Aubin, *Judge Approves $27 Mln Home Depot Data Breach Settlement*, REUTERS (Sept. 26, 2017, 1:25PM), https://www.reuters.com/article/homedepot-settlement/judge-approves-27-mln-home-depot-data-breach-settlement-idUSL2N1M71PK.

139 Jonathan Stempel, *Home Depot Settles Consumer Lawsuit Over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016, 10:33 AM), https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z.

140 Jonathan Randles, *States Investigate Home Depot Data Breach*, LAW 360 (Sept. 9, 2014, 5:30 PM), https://www.law360.com/articles/575613/states-investigate-home-depot-data-breach.

141 Data Security—Cases, FTC, https://www.ftc.gov/datasecurity (last visited Nov. 16, 2017); Randles, *supra* note 140.

Home Depot's failure to take reasonable steps to protect its data, computer experts from within the company have come forward to announce that they warned the company for years of the potential vulnerabilities the company's network faced.[142]

C. Equifax

The most recent company to suffer a high-profile data breach is Equifax. The company suffered a series of data breaches from May to July of 2017.[143] Hackers obtained over 143 million consumers' personal data including Social Security numbers, birth dates, addresses, and driver's license numbers.[144] Hackers accessed Equifax's networks through a web-application vulnerability that was made publicly known in March.[145] Thus, Equifax had over two months to update and patch the web-application vulnerability before the hack took place.[146] Besides the failure to update its software, Equifax is also being widely criticized for the amount of time it took the company to disclose that a breach occurred: six weeks.[147] Although it is too early to tell whether the FTC or any other government agencies will bring an action against Equifax, Congress has held a number of hearings related to the hack.[148] During one of the hearings in which the former CEO of Equifax testified, Congressman Joe Barton stated that

---

[142] Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, N.Y. TIMES (Sept. 19, 2014), https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html (suggesting that Home Depot relied on outdated software to protect its systems and that numerous employees on the data security team left the company over management's failure to acknowledge their concerns).

[143] Jackie Wattles & Selena Larson, *How the Equifax Data Breach Happened: What We Know Now*, CNN TECH (Sept. 16, 2017, 4:06 PM), http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html.

[144] *Id.*

[145] Newman, *supra* note 17.

[146] *Id.*

[147] Turner, *supra* note 3.

[148] Seth Fiegerman & Donna Borak, *Former Equifax CEO Testifies Before Congress*, CNN: MONEY (Oct. 3, 2017, 4:40 PM), http://money.cnn.com/2017/10/03/news/companies/equifax-ceo-congress/index.html; Rebecca Shabad, *Senate Panel Holds Hearing on Equifax, Yahoo Security Breaches*, CBS NEWS (Nov. 8, 2017, 9:59 AM), https://www.cbsnews.com/live-news/senate-panel-holds-hearing-on-equifax-breach-consumer-data-security-live-updates/.

Congress needs to impose "some teeth" at the federal level for regulating data breaches.[149]

D. The Inadequacy of Current Data Breach Laws and Regulations

Ultimately, this review shows that the current federal and state laws and regulations are not effective in preventing data breaches from occurring. The number of data breaches has continued to rise over the past decade.[150] Furthermore, many corporate officers and boards of directors still do not actively participate in overseeing or managing their companies' data privacy practices.[151] As one expert states, "A few very public breaches aside—Target is an example—corporations find it cheaper to spend money on PR campaigns touting good security, weather the occasional press storm and round of lawsuits when they are proven wrong, and fix problems after they become public."[152] The three examples above are proof that Congress needs to reform the current legal landscape regulating data security to incentivize companies to be proactive in implementing reasonable data security practices. Any reforms in the data security realm must create harsher penalties for companies with unreasonable data security practices so that companies no longer view data breaches as a cost of doing business.

IV. A TWO-TRACKED APPROACH TO IMPROVING BUSINESSES' DATA SECURITY PRACTICES

As the number of data breaches continue to rise, more people are starting to advocate for an overhaul of the current legal landscape governing data security.[153] There are a couple of common problems with the current system, including a lack of uniformity creating gaps in the law,

---

[149] *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the Subcomm. Dig. Commerce & Consumer Prot.*, 115th Cong. 45 ll. 21–23 (2017) (statement of Rep. Joe Barton, Vice Chairman, H. Comm. on Energy & Commerce) [hereinafter, Barton Testimony]; Fiegerman & Borak, *supra* note 148.

[150] Lord, *supra* note 48; *see supra* Section II.A.

[151] Noah G. Susskind, Note, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 583–85 (2015).

[152] BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 191–93 (2015).

[153] Barton Testimony, *supra* note 149; Marshall, *supra* note 4, at 106–09; Weinberger, *supra* note 55.

compliance difficulties due to many differing laws, and a reactive rather than proactive approach to improving data protection.[154] To remedy many of these problems, Congress needs to adopt a uniform federal law that preempts state laws governing data privacy. This prevents the headaches for companies that transact business in many different states caused by having to comply with differing state data breach notification laws.[155] In addition, a uniform federal law would replace the current federal approach of industry-specific laws, which creates gaps.[156]

The federal law would start by defining two general categories of information that businesses may obtain: (1) personally identifiable information (PII) and (2) non-personally identifiable information (non-PII). For example, Congress could borrow the definition used by the U.S. Government Accountability Office (GAO) in defining PII for other government agencies. The GAO defines PII as "any information about an individual maintained by an agency . . . that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, . . . [and] any other information that is linked or linkable to an individual."[157] The federal statute could then define non-PII as anything that is not captured by the PII definition. The purpose of having the two categories of information is to encourage corporations to only use non-PII by making the compliance requirements, as discussed below, much less stringent than the requirements for corporations obtaining PII. This adds an extra layer of protection for consumers by reducing the overall amount of PII obtained by a corporation, which in turn lessens the harm to consumers if and when a data breach occurs.

The GAO's definition of PII is suitable for use in a uniform federal law because it is written for a variety of agencies in different industries and is based on the synthesis of numerous definitions of PII in various Office of Management and Budget memorandum.[158] This is

---

154 *See supra* Part II, III.

155 Tschider, *supra* note 61, at 64.

156 *Id.* at 52; Skelton, *supra* note 22, at 305–06.

157 U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-343, INFORMATION SECURITY: PROTECTING PERSONALLY IDENTIFIABLE INFORMATION 5 n.9 (2008) [hereinafter, GAO Report on Information Security].

158 ERIKA MCCALLISTER ET AL., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII), NAT'L INST. OF STANDARDS AND

supported by the definitions use of the broad language "maintained by *an agency*" instead of specifying the particular agencies to which the definition applies.[159] Thus, the GAO's definition of PII is not industry-specific. A broad, non-industry specific definition of PII is needed for the very reasons that the current industry-specific federal laws, mentioned previously, are inadequate at regulating data security: industry-specific laws create gaps.[160]

Congress would also need to authorize the Department of Commerce's National Institute of Standards and Technology (NIST) to promulgate industry standards that businesses must follow to protect their data.[161] The industry standards would vary based on the category of information. Thus, companies obtaining PII would have more stringent standards than companies obtaining only non-PII. The remainder of the statute would then be bifurcated into two tracks: a PII track and a non-PII track.

The NIST is best positioned to establish and monitor cybersecurity standards because its focus is on commerce in general, not a specific industry or business segment.[162] Moreover, the NIST has already established a cybersecurity framework that 30% of businesses follow.[163] In addition, it is projected that close to 50% of businesses will follow this framework by the year 2020.[164] Further, the NIST's industry standards are most likely the least disruptive to the business community, as the NIST formulated its cybersecurity framework in collaboration with the private

---

TECHNOLOGY, U.S. DEP'T OF COM. ES-1, n.6 (2010), https://csrc.nist.gov/publications/detail/sp/800-122/final.

159 GAO Report on Information Security, *supra* note 157, at 5 n.9 (emphasis added).

160 *See supra* Section II.B.

161 NAT'L INST. STAND. TECH., CYBERSECURITY FRAMEWORK, https://www.nist.gov/industry-impacts/cybersecurity (last visited Nov. 16, 2017) [hereinafter Cybersecurity Framework].

162 NAT'L INST. STAND. TECH., NIST MISSION, VISION, CORE COMPETENCIES, AND CORE VALUES, U.S. DEP'T OF COM, https://www.nist.gov/about-nist/our-organization/mission-vision-values (last updated Jan. 26, 2017).

163 Cybersecurity Framework, *supra* note 161.

164 *Id.*

sector.[165] Thus, the private sector is involved in creating the cybersecurity standards that they will have to follow.

The biggest concern with authorizing the NIST to formulate the industry standards is the potential for businesses that collaborate with the NIST to advocate for lower standards so that it is easier for businesses to comply with the law. If this were to occur, one option would be for Congress to amend the enabling authority for the NIST, specifying that it may not collaborate with the private sector in creating cybersecurity standards. Alternatively, Congress could set minimum cybersecurity standards in the uniform federal law and then allow the NIST to add various standards on top of the ones already established in the statute. Overall, the concern with having the NIST collaborate with the private sector in formulating cybersecurity standards may not result in the lowering of those standards. After all, this collaborative process is not all that different from the regulatory process that many federal agencies follow when promulgating their rules.[166]

Under the PII track, the board of directors would be required to form a committee or subcommittee that oversees the company's data security practices.[167] The statute would impose personal liability on the directors who sit on that committee, as well as the corporate officers who are tasked with implementing the company's data security plan. These directors and officers would be liable for any negligent (i.e. unreasonable) data security measures that lead to a data breach.

Within the corporate governance structure, the board should be tasked with monitoring a company's data security practices for a couple of reasons. First, directors owe fiduciary duties to the corporation and its

---

165 NAT'L INST. STAND. TECH, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, U.S. DEP'T OF COM 1 (2014), https://www.nist.gov/document-3766.

166 Section 553(c) of the Administrative Procedure Act states that "the agency shall give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation." 5 U.S.C. § 553(c) (2016).

167 At least some commentators agree that corporate boards should take responsibility in monitoring their companies' cybersecurity risks. *See* Sam Curry, *Boards Should Take Responsibility for Cybersecurity. Here's How to Do It*, HARV. BUS. REV. (Nov. 16, 2017), https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it.

shareholders.[168] One of those duties is the duty of oversight, which falls under a director's broader duty of loyalty.[169] Because data breaches have a direct impact on a company's bottom line,[170] directors are obligated to ensure that their company prevents these breaches to the greatest extent possible. A second reason for holding the board directly accountable for a company's cybersecurity practices is because of its role in appointing corporate officers.[171] The officers of a company are going to be instrumental in monitoring a company's data security practices on a day–to–day level. If an officer fails to meet the level of data security monitoring and protection that the board wishes to achieve, the board can replace that officer.[172]

At first blush, this may seem too harsh. However, the statute would also provide a safe harbor for these individuals. To obtain the safe harbor's protection from personal liability, the company would simply need to follow the industry standards set by the NIST for companies obtaining PII. If the company follows these standards, then these directors and corporate officers could not be held personally liable. A final requirement under this track is that companies obtaining PII would be required to obtain a yearly audit conducted by an independent third-party. This audit would provide an internal mechanism for companies to ensure that they comply with the current industry standards. In addition, the company would need to file the audits with the FTC as proof of compliance with the industry standards that provide the safe harbor from personal liability.

Under the non-PII track, a company would need to follow the industry standards set by the NIST for companies obtaining non-PII data. If a data breach occurs, the company can be held liable under a bad faith standard of liability. This standard of liability is modeled off of a director's duty of oversight as established in *In re Caremark International Derivative*

---

168 Anne Tucker Nees, *Who's the Boss? Unmasking Oversight Liability within the Corporate Power Puzzle*, 35 DEL. J. CORP. L. 199, 208 (2010).

169 *Id.* at 209.

170 *See supra* Part II (discussing that the average cost of a data breach is $7.35 million). Another cost that directors want to avoid is litigation expenses that arise from defending shareholder derivative suits. *See supra* Section III.C.

171 *See* DEL. CODE ANN. tit. 8, § 142(b) (2018).

172 *Id.* §142.

Litigation.[173] Thus, a company under the non-PII track would be liable for a data breach if it had a sustained and systemic failure to exercise reasonable oversight.[174] However, if the directors tasked with overseeing data security or the corporate managers in charge of implementing the company's data security practices knowingly or intentionally violate the industry standards, then they could be held personally liable for any data breach. Finally, there would be no yearly audit requirement for businesses that are only obtaining non-PII. This would reduce the cost of complying with the federal statute and would provide an incentive for companies to only obtain PII if necessary for their business operations. This avoids the costs of a yearly audit and filing requirement.

V. CONCLUSION

The current legal landscape for data privacy and protection has proven inadequate to curb the number of data breaches that companies suffer each year. In the wake of the Equifax data breach, many experts have called on Congress to take action to prevent future data breaches caused by unreasonable corporate behavior. Any future legislation in the area of data security needs to address the current issues that the regulatory, federal, and state laws create, including gaps in the law, compliance headaches for businesses transacting across numerous states, and the reactive nature to preventing data breaches. Ultimately, the proposed uniform federal statute discussed here would remedy these problems and, hopefully, reduce the number of data breaches that occur in the future.

---

[173] *See generally In re* Caremark Int'l, Inc. Derivative Litig., 698 A.2d 959 (Del Ch. 1996).

[174] *Id.* at 971.