BETTER LATE THAN NEVER: BRINGING THE DATA SECURITY REGULATORY ENVIRONMENT INTO THE MODERN ERA

I. INTRODUCTION

If one were to take a walk down the street and ask ten individuals if they had ever been a victim of a large-scale data breach, approximately six out of that ten would indicate that they had been a victim.[1] Americans are extremely wary of large-scale key institutions' ability, such as the government and social media

[1] Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR.: INTERNET & TECH. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

companies, to protect the information that consumers choose to provide or are forced to provide to these organizations.[2] This shared concern is not without basis. Recently, there has been a significant increase in the frequency of data breaches involving millions of personal records, each having significant impact on the victims.[3]

Consider the story of Katie Van Fleet—a Seattle, Washington, resident who became a victim of the recent Equifax breach.[4] Ms. Fleet's self-described nightmare began in September of 2017 when she received a thank-you note for opening a new line of credit.[5] She had no knowledge of how this account was opened.[6] From then on, the gracious thank-you notes continued to roll in from retail stores and other credit agencies.[7] In total, over a dozen unauthorized accounts were opened in Ms. Fleet's name.[8] Alarmed by the flurry activity, Ms. Fleet froze her credit reports and filed a police report.[9] After taking those initial steps, Ms. Fleet retained an attorney and filed a class action suit against Equifax for the recent data breach.[10] Ms. Fleet's story, while extreme, does not exist in a vacuum.

For example, David Anderson had his personal information stolen four times over the span of four years.[11] Specifically, Mr. Anderson's information was stolen during the Target Data Breach, a breach at the University of Maryland, a breach at the Office of Personnel Management, and the Equifax data breach.[12] So far, Mr. Anderson has been lucky enough to avoid suffering any direct financial losses due to the various breaches—others were not so lucky.[13] One

---

2 *See id.* Approximately half of Americans do not trust these organizations to adequately protect their information. *Id.*

3 Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html (collecting reader responses when readers were asked how their lives were impacted by data breaches over the recent span of time).

4 Dominique Mosbergen, *Seattle Woman Says Her Identity Has Been Stolen 15 Times Since Equifax Data Breach*, HUFFPOST (Oct. 30, 2017, 10:18 AM), https://www.huffingtonpost.com/entry/katie-van-fleet-equifax-stolen-identity_us_59f71d08e4b07fdc5fbf782d.

5 *Id.*

6 *See id.*

7 *Id.*

8 *Id.*

9 *Id.*

10 *Id.*

11 Hsu, *supra* note 3.

12 *Id.*

13 *Id.*

individual's credit was harmed to the extent that he was unable to secure a refinanced mortgage, a significant financial roadblock.[14]

Additionally, Janis Barbour's social security number was stolen and utilized to file a fraudulent tax return in Ohio even though she lives in California.[15] Barbour was unaware of this fraudulent activity until the Internal Revenue Service notified her of the inconsistencies in her tax returns.[16] What followed was a nine-month journey during which she had to contact over five different governmental and non-governmental organizations to correct the error.[17]

To combat these various issues, local businesses have taken drastic steps, such as rejecting electronic payments, not utilizing an internet-connected computer, and calling credit card companies to process electronic transactions, to avoid any potential liability.[18]

Data breaches cause a significant impact on both individual and corporate victims. The current regulation system has not evolved in the proper way to deal with the exponential increase in data breaches. Therefore, this Note will explore the current identity authentication process, the underlying causes of data breaches, and the current regulation scheme. Then, this Note will propose a solution to bring the regulation landscape up-to-date with the current cyber security landscape. First, Section II.A. outlines the underlying causes that have led to a significant increase in data breaches. Second, Section II.B. examines the anatomy of a typical data breach—if there is such a thing as a typical data breach. Finally, Section II.C. provides an overview of the applicable statutory regulations and private contractual obligations that attempt to stem the tide of data breaches.

Part III proposes three regulatory reforms designed to address the most significant underlying causes of data breaches. Section III.A. calls for a refined, modernized, and secure replacement for the social security number. Section III.B. proposes an increased standard for privacy policies to allow consumers to make informed decisions about what personal information is shared. Section III.C. calls for Congress to act, and explicitly permit the Federal Trade Commission to regulate the payment card industry through the adoption of the current Payment Card Industry Data Security Standards.

---

14 *Id.*

15 *Id.*

16 *Id.*

17 *Id.*

18 Jim Therrien, *Lawmakers Hear Residents on Data Breaches*, MANCHESTER J. (Nov. 16, 2017, 9:12 AM), http://www.manchesterjournal.com/stories/lawmakers-hear-residents-on-data-breaches,524760.

II. BACKGROUND

Section II.A. will first examine current types of personal information being targeted, why companies are collecting the information, and the problems surrounding the current authentication scheme. Section II.B. then explores the underlying nature of a data breach and the variety of causes. Finally, Section II.C. identifies the current regulation and enforcement scheme available before the breach and the avenues of redress available to victims who have had their information stolen.

A. Problems Surrounding the Current Identity Authentication Scheme in the United States

One well-known principle in the computer science field is Moore's Law.[19] According to Gordon Moore, the observer of Moore's law,[20] chip technology was advancing at such a pace that every other year twice as many transistors could fit on a single chip.[21] Since 1975, Moore's observation has largely held true and, as a result, technology plays a rapidly increasing role in our society.[22] That increasing role has created a ripe opportunity for business to collect and utilize a massive amount of personal data from customers and even from individuals who are not their customers.[23]

Every day, an unimaginable amount of data is generated. According to recent reports, two and a half quintillion bytes[24] of data are generated daily.[25] "To

---

19 Peter Bright, *Moore's Law Really Is Dead This Time*, ARS TECHNICA (Feb. 10, 2016, 8:22 PM), https://arstechnica.com/information-technology/2016/02/moores-law-really-is-dead-this-time/; Tom Simonite, *Moore's Law Is Dead. Now What?*, MIT TECH. REV. (May 13, 2016), https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/.

20 Simonite, *supra* note 19.

21 *Id.*

22 *Id.*

23 *Id.*

24 2,500,000,000,000,000,000 bytes.

25 IBM MARKETING CLOUD, 10 KEY MARKETING TRENDS FOR 2017 AND IDEAS FOR EXCEEDING CUSTOMER EXPECTATIONS 3 (2017), https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reports-wrl12345usen-20170719.pdf. A byte is "a unit of computer information or data-storage capacity that consists of a group of eight bits and that is used especially to represent an alphanumeric character." *Byte*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/byte (last visited Sept. 14, 2018). Originally, byte was a unit for measuring character data, but, over time, a byte became the fundamental measurement for all data storage. *Byte*, TECHTERMS, https://techterms.com/definition/byte (last updated Nov. 30, 2011). Because a byte is an extremely small unit of data measurement, various

put that into perspective, 90 percent of the data in the world today has been created in the last two years alone . . . ."[26] Additionally, the amount of data generated daily is equivalent to approximately 50 million high-capacity Blu-ray discs.[27] The daily data produced is exponentially increasing, and some estimate that by the year 2020, 40 zettabytes[28] of data will be created on a daily basis.[29]

Most often, when individuals hear of a data breach, they assume, as often is the case, that their credit card information has been stolen.[30] One of the more well-known data breaches was when a large amount of credit card information was stolen from Target Corporation's network.[31] In that attack, the information of approximately 110 million customers—including debit and credit card numbers—was stolen from the retailer's system.[32] Since then, there has been an increasing number of large scale breaches, and the impact of the breaches has only grown more concerning.[33]

Within the last fifteen years, there has been a significant change in how non-cash payments are used and handled.[34] The once-reigning king of non-cash payments, handwritten checks, has now been dethroned by various electronic payment methods.[35] From its peak in 1995, the use of checks has been steadily declining each year.[36] Currently, the leading non-cash payment method is debit card payments, with a total of 69.5 billion payments in 2015 and a value of $2.56

prefixes are attached—for example, "mega-"and "tera-"—to represent an exponential increase in the number of bytes the storage device is capable of storing. *See id.*

26 IBM MARKETING CLOUD, *supra* note 25, at 3.

27 *Id.*

28 40,000,000,000,000,000,000,000 bytes.

29 Daniel Price, *Infographic: How Much Data Is Produced Every Day?*, CLOUDTWEAKS (Mar. 17, 2015), https://cloudtweaks.com/2015/03/how-much-data-is-produced-every-day/.

30 *Data Breaches 101: How They Happen, What Gets Stolen, and Where it all Goes*, TREND MICRO (Oct. 23, 2015), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

31 *See In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1154 (D. Minn. 2014).

32 *Id.* at 1157.

33 *2015 Data Breaches*, IDENTITY THEFT RESOURCE CTR. (Jan. 25, 2016), https://www.idtheftcenter.org/2015-data-breaches/; *see also ITRC Breach Statistics 2005 – 2016*, IDENTITY THEFT RESOURCE CTR. (2017), https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf (compiling data breach statistics from 2005 through 2016 and categorizing based on industry affected and category of breach).

34 FED. RESERVE SYS., THE FEDERAL RESERVE PAYMENTS STUDY 2016 1 (2016), https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf.

35 *Id.*

36 *Id.* at 2.

trillion.[37] Following debit card payments, credit card payments were utilized in 33.8 billion transactions in 2015 with a total value of $3.16 trillion.[38] Next, Automatic Clearing House payments were utilized in 23.5 billion transactions in 2015, with a relatively large value of $145.30 trillion. Overall, the frequency of non-cash payments has increased at an annual rate of 5.3% between 2012 and 2015 and will likely continue to increase at a similar rate.[39] Additionally, non-cash payments are going through a technological evolution to enable a more secure transaction.[40] However, the adoption of this technology has been gradual, and the majority of non-cash payments are still a significantly attractive target for credit and debit card fraud.[41]

While non-cash payment information is often the target of attacks, the individuals responsible for breaches are also stealing other personally identifiable information because of the ease of using the stolen information.[42] According to the United States Office of Management and Budget, personally identifiable information ("PII") is any information that can be used, alone or in conjunction with other information, to uncover an individual's identity.[43] Therefore, PII can include a broad range of identifiers such as date of birth, ZIP code, driver's license number, phone number, and much more.[44]

Furthermore, approximately 87% of the United States' population can be identified with a mere three pieces of information—gender, ZIP code, and date of birth.[45] Companies can be driven to collect this type of information for a

---

37 *Id.* at 3.

38 *Id.*

39 *Id.* at 2.

40 This has included the adoption of debit card and credit card with chip and signature technology or chip and pin technology. *See id.* at 7. Without the proper hardware updates, merchants are unable to utilize this more-secure method, so they default to the less-secure magnetic strip payment method. *See id.*

41 *Id.*

42 *See, e.g.*, *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

43 *Rules and Policies - Protecting PII - Privacy Act*, U.S. GEN. SERVS. ADMIN. (Oct. 31, 2014), https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act. "The term 'PII,' as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." *Id.*; *see also* John Stringer, *Protecting Personally Identifiable Information: What Data Is at Risk and What You Can Do About It*, SOPHOS 2 (2011), https://www.sophos.com/en-us/medialibrary/pdfs/other/sophosprotectingpii.pdf.

44 Stringer, *supra* note 43, at 2.

45 *See generally* Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, PALO ALTO RES. CTR. (2006), https://crypto.stanford.edu/~pgolle/papers/census.pdf

variety of reasons.[46] For example, a consumer may provide information to sign up for a service, but most often a company will request unnecessary additional information to advance their marketing programs.[47]

Perhaps the most heavily-guarded—holy grail like—of all personal information in existence today is the social security number. Social security identification numbers are so highly-regarded because the numbers are unique and often remain with a person for life.[48] Furthermore, social security numbers are provided to all United States citizens, and sometimes to noncitizens, by the Social Security Administration.[49] Therefore, the social security number is uniquely situated to serve as an identifier.[50]

Originally created in 1936, the social security card was only intended to serve as an identifier for social security programs.[51] However, over time, organizations recognized that the social security number could easily be used for identification.[52] Perhaps the most significant shift for the social security number occurred in 1961 when the Internal Revenue Service ("IRS") began using the social security number as a method for tax payer identification.[53] Since then, all transactions involving IRS reporting required the attachment of an individual's social security number.[54] Additionally, credit card applications often require a social security number for the financial institution to identify the applicant.[55] In comparison, other countries seem to rely less on credit than United States consumers and do not place the same amount of emphasis on a social security-type number like United States-based companies do.[56]

(evaluating the study based on the 1990 census that identified this provision and ultimately concluding that only 63% percent of the population could be identified through this).

46 Stringer, *supra* note 43, at 1.

47 *Id.*

48 *See generally* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 95–100 (2001) (discussing how the social security card is utilized to verify the identity of individuals in conjunction with the use of other known information in common transactions such as retail credit accounts).

49 *See* SOC. SEC. ADMIN., YOUR SOCIAL SECURITY NUMBER AND CARD, PUBLICATION NO. 05-10002 (2017).

50 LoPucki, *supra* note 48, at 95–100.

51 University of San Diego Center for Public Interest Law, *How to Keep Your Personal Information Personal: Tips from the Privacy Rights Clearinghouse*, 14 CAL. REG. L. REP. 1, 5 (1994).

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.*

56 *See, e.g.*, CREDIT CARD APPLICATION FORMS EXPLAINED, UKCREDITCARDS.COM, http://uk.creditcards.com/assets/documents/credit-card-application-forms-explained.pdf (last

For example, Canada has recognized the weaknesses of having a national identification number similar to the social security number.[57] In 2004, a privacy law went into effect that explicitly prohibited Canadian companies and organizations from requiring the production of a citizen's Social Insurance Number ("SIN"), which is the Canadian equivalent of a social security number.[58] This adoption was a significant departure from the prior scheme where businesses were permitted to collect the SIN in order to identify the individual and to make credit decisions.[59] To enact this significant shift, the Canadian government focused on working with private businesses to ensure that there would not be a negative impact on their business.[60] Through this cooperative effort, the privacy act did not completely bar organizations from collecting information, but it required proper notice of any personal data usage and free consent for the collection of a SIN.[61] However, after the privacy act went into effect, some businesses experienced growing pains.[62] For example, one business was sanctioned by an administrative agency for not properly formatting the company's credit application form and for not stating that providing a SIN was optional.[63] Canada's enactment of the Personal Information Protection and Electronic Documents Act provides an example of how a country has moved from the singular key to the kingdom—a national identification number with a wide variety of uses—to a limited national identification number.

visited Oct. 5, 2018); *Identification*, NZ TRANSPORT AGENCY, https://www.nzta.govt.nz/driver-licences/getting-a-licence/identification/ (last visited Oct. 5, 2018).

57 *See generally* David T.S. Fraser, *New Rules for Using Social Insurance Numbers: Privacy Legislation Places Limits on SIN*, MCINNES COOPER (2003), http://www.privacylawyer.ca/privacy/piepda_and_social_insurance_numbers.pdf (discussing the adoption and application of the new privacy law).

58 "4.3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes." Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

59 Fraser, *supra* note 57, at 1.

60 Ruwantissa Abeyratne, *Attacks on America—Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada*, 67 J. AIR L. & COM. 83, 109 (2002).

61 *Id.* at 111.

62 *See* Fraser, *supra* note 57, at 2.

63 As for the matter of providing SINs, the Commissioner referred to another recent finding with respect to a different bank's credit card application form. In that case, the focus was on the fact that this form did not clearly indicate that providing the SIN for identification purposes was optional. It was determined that the bank had not made a reasonable effort to ensure that the customer was adequately informed of this and, as a result, was not obtaining valid, meaningful consent. Fraser, *supra* note 57, at 1.

B. Anatomy of a Data Breach

To begin, no data breach between organizations, or even a repeated breach within the same organization, is similar for a number of reasons. For example, a breach could impact a limited system within the network, resulting in minimal impact, or, conversely, the breach could spread undetected through the entire network.[64] This Section will address the underlying cause of data breaches and will discuss some well-known incidents to highlight the breach's effect and how an organization should respond.

As a general matter, data breaches can be categorized into three groups based on the nature of the intrusion: well-meaning insiders, targeted attacks, and malicious insiders.[65] Each individual subgroup has different characteristics that give rise to the data breach and the causes are often intermingled between the different categories.[66]

The first group of data breaches, those involving well-meaning insiders, occur when an employee opens the door for nefarious actors to infiltrate a system.[67] One common example of this is a phishing attack that may be directed at a specific individual.[68] In order to accomplish this infiltration, the attacker typically creates a legitimate looking e-mail or website and directs the e-mail towards a business's employees.[69] While not solely designed to infiltrate the system, the phishing attack is designed to passively collect an employee's credentials that will later be used by the attacker.[70] Another version of a well-meaning insider attack occurs when an employee does not follow the organization's established data security policy.[71] For example, if an employee has created a file that contains highly sensitive information but then fails to take the proper steps to secure the data, that employee has created a massive risk.[72] Additionally, employees are a weak link because humans are vulnerable to social

---

64 *See* Morgan O'Mara, *Different Types of Data Breaches*, SHRED NATIONS, https://www.shrednations.com/2015/08/different-types-of-data-breaches/ (last updated Jan. 29, 2018).

65 SYMANTEC CORP., ANATOMY OF A DATA BREACH: WHY BREACHES HAPPEN AND WHAT TO DO ABOUT IT 2–6 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-anatomy_of_a_data_breach_WP_20049424-1.en-us.pdf.

66 *Id.*

67 *Id.* at 2–3.

68 Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 290 (2006).

69 *Id.*

70 *Id.*

71 *Id.*

72 SYMANTEC CORP., *supra* note 65, at 6–7.

engineering.[73] Through social engineering, an employee may unknowingly and willingly give an outside individual access to the system by sharing a password or providing the attacker with enough information to gain access.[74]

The second group, targeted attacks, consists of attacks where companies must engage in active prevention to ensure that a weakness is not capitalized on by an attacker.[75] This type of attack is dissimilar to the well-meaning insider attack because the attackers are taking active steps to exploit program vulnerabilities.[76] One potential vulnerability that attackers might exploit is a security hole located in older software that has not been updated.[77] In fact, this is a frequent avenue of attack because corporate entities often utilize legacy software and sometimes do not update the underlying operating system with new security updates.[78] In addition, attackers may utilize a targeted attack in hopes of obtaining information that will grant the attackers access to a larger system.[79] For example, an attack that led to a larger breach occurred when the attackers infiltrated a large retail store's network due to the breach of a contractor's network.[80] After obtaining access to the contractor's network, the attackers discovered credentials that granted access to the retail store's network.[81] Thereafter, the attackers were able to freely move about the store's network to install register-based malware because there was no system in place to separate the different network functions.[82] Those compounded failures resulted in the loss

---

73 *See generally* Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SYMANTEC CORP. (Dec. 18, 2001), https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics (discussing the various social engineering methods that attackers utilize to infiltrate the business networks).

74 Hahn & Layne-Farrar, *supra* note 68, at 290–91.

75 SYMANTEC CORP., *supra* note 65, at 3–4.

76 *Id.*

77 *Id.*

78 *See* Dan Woods, *Why You Must Build Cybersecurity Into Your Applications*, FORBES (Apr. 20, 2017, 6:49 AM), https://www.forbes.com/sites/danwoods/2017/04/20/why-you-must-build-cybersecurity-into-your-applications.

79 *Id.*

80 Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBSONSECURITY (Feb. 5, 2014), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ [hereinafter *Hackers Broke in Via HVAC Company*].

81 *Id.*

82 Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBSONSECURITY (Sept. 21, 2015), https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/ [hereinafter *Inside Target Corp.*].

of approximately 110 million customer records, including 40 million card numbers.[83]

The final, largest category of data breaches, is the malicious insider. A malicious insider is an employee who has been granted appropriate access levels but uses that access for their own personal gain or for a competitor's gain.[84] Employees at risk for this type of behavior include recently-terminated employees, career building employees, employees engaged in industrial espionage, and employees who are actively involved in white collar crime.[85] Each category of employees poses a different challenge to address in order to prevent data breaches, and there is no clear answer on how to prevent an employee from sabotaging their employer.[86] However, an employer can take active steps, such as conducting background checks, monitoring employee behavior, limiting access to sensitive information, and educating employees to limit the risk of a malicious insider breach.[87]

One particular data breach that highlights the consequences of an organization failing to take proper steps to prevent an intrusion and subsequent breach is the 2014 Home Depot data breach.[88] As a result of the data breach, Home Depot was sued by multiple parties, including various financial institutions that suffered significant losses because they were forced to issue new credit cards and reimburse consumers for any financial loss.[89] In addressing Home Depot's motion to dismiss, the court discussed the variety of factors that contributed to the data breach.[90] Home Depot's troubles began in 2008 when multiple employees informed their supervisors that "the computer systems were 'easy prey for hackers' and that they could be breached by anyone with 'basic internet skills.'"[91] Furthermore, in 2009, employees once again warned that Home Depot was not using effective security measures because the company

---

83 *See In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1307 (D. Minn. 2014); *Inside Target Corp.*, *supra* note 82.

84 SYMANTEC CORP., *supra* note 65, 5–6.

85 *Id.*

86 *Id.*

87 Marcell Gogan, *Insider Threats as the Main Security Threat in 2017*, TRIPWIRE (Apr. 11, 2017), https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/.

88 *See In re* The Home Depot, Inc., Customer Data Sec. Breach Litig., 1:14-MD-2583-TWT, 2016 WL 2897520 at *1 (N.D. Ga. May 18, 2016) (granting in part and denying in part The Home Depot Inc.'s motion to dismiss).

89 *Id.*

90 *Id.*

91 *Id.*

failed to encrypt sensitive customer data.[92] Home Depot, instead of fixing the issue, chose to terminate the employee who specifically warned of a system vulnerability; addressing the vulnerability likely would have limited the impact of the data breach that did occur.[93] In 2012, Home Depot hired a computer engineer to oversee the security of its stores, but the engineer was sentenced to prison in 2014 for sabotaging the computer systems at a previous place of employment.[94] Overall, Home Depot fostered a culture where data security fell behind all other priorities and the business suffered as a result.[95] Specifically, management instructed employees not to fix security deficiencies and warned the employees that their efforts were futile because the company would not spend any money to make the necessary improvements.[96]

The perfect storm of failures came to a head in April of 2014 when hackers were able to gain access to Home Depot's system after stealing a contractor's credentials.[97] Once the hackers were in the system, they were able to successfully install malware on the store's self-checkout terminals without raising any alarms.[98] The hackers then collected customers' debit and credit card information from the terminals for approximately five months before Home Depot was notified of the breach in the system.[99] By the time Home Depot was aware of the breach, approximately 50 million pieces of consumer information were stolen and placed for sale on the black market.[100] Home Depot eventually

92 *Id.*

93 *Id.*

94 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.

95 *In re* The Home Depot, Inc., 2016 WL 2897520, at *1.

96 *Id.*

97 *Id.* at *2.

98 *Id.*

99 *Id.*

100 Home Depot was notified by the United States Secret Service on Sept. 2, 2014, that its systems had been breached. *Id.* at *2. The Secret Service is often the first investigative agency to notify corporations of large scale data breaches because the agency is responsible for the investigation of large scale financial crimes. *See The Investigative Mission*, U.S. SECRET SERV., https://www.secretservice.gov/investigation/ (last visited Sept. 24, 2018). Additionally, card issuers and banks are often the first to notice and link the large-scale fraud to a specific company as the stolen information is sold and used for fraudulent transactions. *See* Kimberly Palmer, *How Credit Card Companies Spot Fraud Before You Do*, U.S. NEWS (July 10, 2013, 10:00 AM), https://creditcards.usnews.com/how-credit-card-companies-spot-fraud-before-you-do (discussing the various monitoring tools that credit card companies utilize to detect if a card has been compromised).

settled all suits related to the 2014 data breach for approximately $179 million between the consumer classes and the financial institutions.[101]

Another infamous data breach occurred in the fall of 2013 during Target Corporation's busiest time of the year.[102] Similar to Home Depot, Target's system was breached when the attacker infiltrated an outside vendor who had remote access to Target's computer system.[103] Subsequently, the attacker obtained access to Target's payment processing system and installed a program designed to steal payment card information.[104] Prior to the breach being discovered, the attackers were able to steal approximately 110 million customer records, including 40 million debit and credit card numbers.[105] During Target's post-breach review, the company identified several areas, such as weak passwords and outdated security patches, that impacted the scale of the breach.[106] In the aftermath of the breach, Target was sued by both consumers and banks who suffered losses due to the data breach.[107] As a result of the various lawsuits, Target has paid out approximately $116 million through various settlements with card issuers, states, and individual consumers.[108]

Finally, private companies are not the only organizations that can fall victim to a data breach because of an organizational failure. In fact, governmental entities may be more susceptible to an organizational failure that results in a data breach. One recent example is the 2016 breach where attackers obtained access to the Securities and Exchange Commission's ("SEC") system known as

---

101 Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, FORTUNE (Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks/; *see also* Jonathan Stempel, *Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016, 11:33 AM), https://www.reuters.com/article/us-home-depot-breach-settlement/home-depot-settles-consumer-lawsuit-over-big-2014-data-breach-idUSKCN0WA24Z.

102 *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1307 (D. Minn. 2014).

103 TERI RADICHEL, SANS INST. INFOSEC READING ROOM, CASE STUDY: CRITICAL CONTROLS THAT COULD HAVE PREVENTED TARGET BREACH 2 (2014), https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

104 *Id.*

105 *In re Target Corp.*, 64 F. Supp. 3d at 1307; *Inside Target Corp.*, *supra* note 82.

106 *Inside Target Corp.*, *supra* note 82.

107 *In re Target Corp.*, 64 F. Supp. 3d at 1307.

108 *See* Shan Li, *Target Reaches Deal with Visa over 2013 Data Breach*, L.A. TIMES (Aug. 18, 2015, 12:10 PM), http://www.latimes.com/business/la-fi-target-breach-settlement-20150818-story.html; Samantha Masunaga, *Target Will Pay $18.5 Million in Settlement with States over 2013 Data Breach*, L.A. TIMES (May 23, 2017, 3:00 PM), http://www.latimes.com/business/la-fi-target-credit-settlement-20170523-story.html.

Edgar.[109] Edgar is an automated system that has been the sole method for companies filing required forms with the SEC since 1996.[110] Because companies are required to file a wide variety of forms that often contain sensitive information about companies' inner workings, Edgar is an appealing target to attackers who wish to gain insight to a company's future financial events.[111] Knowing this, the SEC continually ignored warnings from the Government Accountability Office ("GAO").[112] By ignoring the GAO's recommendations, the SEC did not properly encrypt the documents stored on Edgar and, when the hackers obtained access, they were able to read the stored documents without restriction.[113] In response, the SEC said it was continuing to investigate a report from the GAO indicating that, at the end of the 2016 fiscal year, the SEC still had not addressed twenty-six recommendations to improve the SEC's information security programs.[114]

C. Current Regulatory System

This Section will provide an overview of the main data security regulatory sources. First, this Section will discuss the Payment Card Industry Data Security Standards, a set of contractually based standards businesses that accept credit card payments must adhere to. Next, this Section provides an overview of State consumer protection law that typically requires consumer notification and free credit monitoring in the event of a data breach. Finally, this Section discusses the Federal Trade Commission and its authority to protect consumer's information prior to and in the event of a breach.

1. Self-Regulation: The Payment Card Industry Data Security Standards Framework

In today's world, when we think of data breaches we often think of our credit card information being stolen from a retailer—that is with good reason

---

109 Renae Merle, *SEC Ignored Years of Warnings About Cybersecurity Before Massive Breach*, WASH. POST (Oct. 24, 2017), https://www.washingtonpost.com/business/economy/sec-ignored-years-of-warnings-about-cybersecurity-before-massive-breach/2017/10/24/7e7507d0-adf7-11e7-be94-fabb0f1e9ffb_story.html.

110 *Important Information About EDGAR*, U.S. SEC, https://www.sec.gov/edgar/aboutedgar.htm (last modified Feb. 16, 2010).

111 Merle, *supra* note 109.

112 *Id.*; *see* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-469, SEC IMPROVED CONTROL OF FINANCIAL SYSTEMS BUT NEEDS TO TAKE ADDITIONAL ACTIONS 4–6 (2017) [hereinafter SEC IMPROVED CONTROL], https://www.gao.gov/assets/690/686192.pdf.

113 Merle, *supra* note 109.

114 SEC IMPROVED CONTROL, *supra* note 112.

because retailers have been the victims of some of the most significant data breaches.[115] However, most people would be surprised to know that the credit card industry, with respect to transaction security, is largely self-regulated.[116] There are many reasons that the industry has remained self-regulated, but a potentially straight forward answer is the complexity of the system.[117] When addressing a data breach, the Southern District of Texas described the credit and debit card payment system as follows:

> Every day, merchants swipe millions of customers' payment cards. In the seconds that pass between the swipe and approval (or disapproval), the transaction information goes from the point of sale, to an acquirer bank, across the credit-card network, to the issuer bank, and back. Acquirer banks contract with merchants to process their transactions, while issuer banks provide credit to consumers and issue payment cards. The acquirer bank receives the transaction information from the merchant and forwards it over the network to the issuer bank for approval. If the issuer bank approves the transaction, that bank sends money to cover the transaction to the acquirer bank. The acquirer bank then forwards payment to the merchant.[118]

To help ensure the security of this complicated system, the various card issuers[119] banded together and formed the Payment Card Industry ("PCI") Security Standards Council.[120] This organization is responsible for establishing and for updating, as needed, the Payment Card Industry Data Security Standards ("PCI-DSS").[121] The PCI-DSS has its own strengths and weaknesses that may affect how secure the credit and debit card processing system is.[122]

---

115 *See supra* Part II.B.

116 *About Us*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/about_us/ (last visited Sept. 24, 2018).

117 *See id.*

118 *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1307 (D. Minn. 2014) (citing *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 574 (S.D. Tex. 2011) (footnote omitted), *rev'd in part sub nom*; *see also* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013)).

119 The founding members of the PCI Security Standards Council are American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. *About Us*, *supra* note 116.

120 *Id.*

121 Rebecca Weinstein, Note, *Cybersecurity: Getting Beyond the Technical Compliance Gaps*, 19 N.Y.U. J. LEGIS. & PUB. POL'Y 913, 927 (2016).

122 *Id.*

In order to comply with the PCI-DSS, businesses that accept electronic payments must pass a scheduled and announced audit once per year in addition to self-certification steps throughout the year.[123] Furthermore, if a business conducts a significant number of electronic payments, the business must hire an outside consultant to conduct an independent inspection of the business's point of sale system.[124] However, if a business only conducts a small number of transactions a year, then the business can conduct a self-assessment to evaluate its compliance with the PCI-DSS.[125] In operation, the PCI-DSS has twelve individual requirements that are designed to help payment card processors achieve six main goals.[126] Within each individual requirement, the standards suggest specific action items a company can and should take to secure the company's network.[127] While not exhaustive, the standards are designed to ensure a basic level of security for the organization.[128] However, companies have often treated the PCI-DSS assessments as a once-a-year checklist to ensure compliance and, ultimately, the company's system may be neglected during the rest of the year.[129]

---

123 *Id.*

124 *Id.* at 928.

125 PCI SECURITY STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE: UNDERSTANDING THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 3.2, 10 (2016), https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf.

126 *Id.* at 9. The twelve requirements include:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Id.

127 *Id.* at 11–24.

128 *Id.* at 4.

129 Weinstein, *supra* note 121, at 929.

2. Limited Protection: Consumer Protection Statutes

Currently, there are forty-seven states that require companies and organizations that collect personal information to notify individuals if a breach compromised the security of personally identifiable information.[130] Furthermore, twenty-three states—including California, Maryland, and New York—require companies to notify the state's Attorney General when there has been a breach that compromised personally identifiable information.[131] The specific criteria requiring notification varies from state to state but ranges from zero to one thousand individuals' personal information being breached.[132]

In West Virginia, two separate statutes contained in the West Virginia Consumer Credit and Protections Act relate to data breaches and consumer rights—the Breach of Security of Consumer Information and the Theft of Consumer Identity Protections.[133] Both statutes encompass different areas and provide different protections.

The Breach of Security of Consumer Information statute requires organizations to provide notice to West Virginia consumers when their unencrypted personal information has been compromised.[134] Unlike some other states, organizations that have suffered a data breach are required to provide notice to West Virginia consumers even if a single West Virginia consumer's unencrypted information was exposed through the breach.[135] Furthermore, the notice must be provided without unreasonable delay.[136] The Breach of Security of Consumer Information statute also requires that organizations inform individual consumers as to the categories of information that were accessed by the unauthorized individuals, methods for the consumer to learn what types of information the organization maintained, and contact information for the three credit bureaus with instructions on how to place a freeze on the consumer's credit reports.[137] If a covered organization fails to comply with the notice requirements,

130 J. Jasen Eige & Katherine Schroth, *State Attorneys General Play Growing Data Privacy Role*, LAW360 (Jan. 10, 2017, 5:53 PM), https://www.law360.com/articles/879583/state-attorneys-general-play-growing-data-privacy-role.

131 *Id.*

132 *Id.*

133 *See* W. VA. CODE ANN. § 46A-2A-101–105 (West 2018); W. VA. CODE ANN. § 46A-6L-101–105 (West 2018).

134 *See* W. VA. CODE ANN. § 46A-2A-102(a) (West 2018).

135 *Id.*

136 *Id.* Notice may be delayed if law enforcement requests the company delay providing notice because the notice may obstruct an ongoing investigation or create a risk to national security. *See Id.* § 46A-2A-102(e).

137 *Id.*§ 46A-2A-102(d).

the West Virginia Attorney General may bring an action with a potential penalty of up to $150,000 if the organization engaged in a "course of repeated and willful violations."[138] Recently, the West Virginia Attorney General has had minor involvement responding to data breaches.[139] The Attorney General joined a lawsuit with forty-seven other states to seek damages from the Target Data Breach.[140] The parties eventually entered into a settlement with Target that required the company to develop an information security program and to maintain an appropriate level of encryption for consumer data.[141]

West Virginia's data breach notification law differs from the law in some other states in one major way—West Virginia consumers have no private right of action.[142] Therefore, the West Virginia consumer must rely on the Attorney General to protect their rights under the notification law.[143] However, the Attorney General's office wears a multitude of different hats.[144] Therefore, if the data breach and subsequent failure to provide notification is not significant, the Attorney General may not pursue the full extent of all remedies. Additionally, the money recovered from a settlement reached may not directly benefit the consumers that suffered the original harm from the data breach.[145]

The second West Virginia statute designed to protect West Virginia consumers from the effects of data breaches is the article of the West Virginia Consumer Credit and Protection Act entitled "Theft of Consumer Identity Protections."[146] While not directly related to the detection, prevention, or notification of data breaches, this statute is important in minimizing the ill effects

---

138 *Id.* § 46A-2A-104(b).

139 Chris Dickerson, *West Virginia to Get $200K in Target Data Breach Settlement*, W. VA. REC. (May 24, 2017), https://wvrecord.com/stories/511119327-west-virginia-to-get-200k-in-target-data-breach-settlement.

140 *Id.*

141 *Id.*

142 *Compare* W. VA. CODE ANN. § 46A-2A-104(b) (West 2018) (stating that "the Attorney General shall have exclusive authority to bring action"), *with* D.C. CODE § 28-3853(a) (2018) (stating that any "resident injured . . . may institute a civil action") *and* N.H. REV. STAT. ANN. § 359-C:21 (West 2018) (stating that "[a]ny person injured . . . may bring an action for damages and for such equitable relief").

143 *See* W. VA. CODE ANN. § 46A-2A-104(b) (West 2018).

144 *See Mission of the Attorney General*, W. VA. ATT'Y GEN.'S OFF., https://ago.wv.gov/about/Pages/default.aspx (last visited Sept. 20, 2018).

145 *See* Kyla Asbury, *House Bill to Limit AG's Use of Settlement Funds Passes 90-7*, W. VA. REC. (Feb. 14, 2018), https://wvrecord.com/stories/511344627-house-bill-to-limit-ag-s-use-of-settlement-funds-passes-90-7 (discussing recent efforts to reform the Attorney General's settlement fund and describing how the Attorney General has already returned $39 million to the state legislature from litigation settlements).

146 W. VA. CODE ANN. § 46A-6L-101–105 (West 2018).

of any data breach that affects consumers.[147] Under this statute, credit reporting agencies are required to allow consumers to prevent their credit report from being distributed to a third party.[148] By mandating that companies offer this service, the state empowers consumers to prevent and stop any potential damage that could occur as a result of a data breach.[149] Freezing a consumer's credit report effectively stops the majority of financial loss related to identity theft because it is exceedingly difficult for anyone other than the consumer to open an account during the freeze.[150] If a credit reporting agency were to negligently violate the credit freeze, a consumer would be entitled to file suit seeking to recover actual damages along with reasonable attorney's fees.[151]

3. The Last Resort: The Federal Trade Commission

The Federal Trade Commission is tasked with protecting American consumers by "preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process . . . ."[152] With that goal in mind, the Commission has become one of the leading regulatory bodies addressing data privacy and data breaches.[153] The Commission has taken multiple approaches toward addressing data privacy, such as setting out aspirational guidelines for companies to create security protocols that fit the needs of their business.[154] Additionally, the Commission has initiated approximately sixty lawsuits against organizations that suffered a breach and did not adequately protect consumer information.[155]

To bring enforcement actions against companies for data breaches, the Commission relies upon Section 5 of the Federal Trade Commission Act of

147 *See Credit Freeze FAQs*, FED. TRADE COMMISSION, https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs (last updated Sept. 2018).

148 W. VA. CODE ANN. § 46A-6L-102 (West 2018).

149 *See id.*

150 *Credit Freeze FAQs*, *supra* note 147.

151 W. VA. CODE ANN. § 46A-6L-104 (West 2018).

152 *About the FTC*, FED. TRADE COMMISSION https://www.ftc.gov/about-ftc (identifying the agency's mission statement) (last visited Sept. 20, 2018).

153 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 604 (2014).

154 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

155 FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2016 (2016), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf.

1914.[156] In Section 5, Congress declared that all deceptive or unfair methods of competition to be unlawful.[157] Recently the Commission has interpreted this section as granting power for the Commission to monitor and regulate a company's unfair or deceptive data security practices.[158] Further, the Commission is permitted to determine if a company's actions fall under the unfair or deceptive prongs of Section 5 and take the action the Commission determines to be appropriate.[159]

i. Enforcement Under Section Five's Deceptive Prong

First, the Commission can take action against organizations under the deceptive prong of Section 5.[160] To establish a violation of the deceptive prong, the Commission must show that the company's business practice "is likely to mislead consumers acting reasonably under the circumstances."[161] A common occurrence is that this type of action is instituted when an organization violates its own terms of service, violates its privacy policy, or utilizes data in an unauthorized manner.[162]

For example, in 2015, the Commission initiated an action against the operators of the Ashley Madison dating website.[163] Prior to the complaint being filed, the dating website suffered a significant data breach that affected approximately thirty-six million consumers from 46 different countries.[164] In the

156 Federal Trade Commission Act of 1914 § 5, 15 U.S.C. § 45 (2018).

157 *Id.* § 45(a)(1).

158 *See* Peter S. Frechette, Note, *FTC v. LabMD: FTC Jurisdiction over Information Privacy Is "Plausible," but How Far Can It Go?*, 62 AM. U. L. REV. 1401, 1402 (2013).

159 *See* 15 U.S.C. § 45.

160 *See* Peter S. Frechette, *supra* note 158, at 1404.

161 FTC v. Stefanchik, 559 F.3d 924, 928 (9th Cir. 2009) (discussing the standard that the Commission must meet to show deception).

162 Amanda R. Moncada, Note, *When A Data Breach Comes a-Knockin', the FTC Comes a-Blockin': Extending the FTC's Authority to Cover Data-Security Breaches*, 64 DEPAUL L. REV. 911, 918 (2015); *see also* Complaint for Permanent Injunction and Other Equitable Relief at 3–7, FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf (initiating action against Ashley Madison because the company used user profiles in an unauthorized manner).

163 *See* Complaint for Permanent Injunction and Other Equitable Relief at 3–7, FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf.

164 *See* Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. TIMES (Aug. 19, 2015), https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html; *see also* Jonah Bromwich, *Ashley Madison Users Face Threats of Blackmail*

complaint, the Commission claimed that the website's operators deceived their consumers on a multitude of different fronts.[165] Some of the alleged failures included the lack of a written organizational information security policy and the failure to implement access controls.[166] Combined with those failures, the website operators further held the website out, both implicitly and explicitly, as being secure.[167] Additionally, the website further deceived consumers by listing a "data security seal" on the website even though the service had never received a "Trusted Security Award."[168]

As a result of the dating website's actions, the Commission investigated and took action against the owners for misrepresenting the website's security.[169] To settle the lawsuit, the Commission and Ashley Madison entered into a consent decree.[170] Under the consent decree, Ashley Madison agreed to no longer misrepresent the service's security features, to implement a data security program designed to reasonably protect the users, and to perform biennial third-party security assessments.[171] Additionally, Ashley Madison agreed to pay approximately ten million dollars in compensation to the Commission.[172]

ii. Enforcement Under Section Five's Unfair Prong

Next, under the unfair practices prong, the Commission has faced pushback from organizations the Commission attempts to hold accountable under Section 5.[173] The Commission most often utilizes the unfairness prong when the Commission determines that an organization has failed to adequately

and Identity Theft, N.Y. TIMES, (Aug. 27, 2015), https://www.nytimes.com/2015/08/28/technology/ashley-madison-users-face-threats-of-blackmail-and-identity-theft.html (explaining additional data security concerns resulting from the Ashley Madison data breach).

165 Complaint for Permanent Injunction and Other Equitable Relief at 3–7, FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf.

166 *Id.* at 9.

167 *Id.* at 8.

168 *Id.* at 14.

169 *Id.* at 1; *see also* Mike McPhate, *Ashley Madison Faces F.T.C. Inquiry Amid Rebranding*, N.Y. TIMES (July 5, 2016) https://www.nytimes.com/2016/07/06/business/ashley-madison-ftc-rebranding.html.

170 Stipulated Order for Permanent Injunction and Other Equitable Relief at 1, FTC v. Ruby Corp., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161214ashleymadisonorder1.pdf.

171 *Id.* at 3–7.

172 *Id.* at 7.

173 Frechette, *supra* note 158, at 1405–06.

protect the consumers' personally identifiable information the organization has collected.[174] To prevail under this prong of Section 5, the Commission must show that the unfair business practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[175] To meet this burden, the Commission must show that the organization's practice created significant monetary, safety, or health risks for consumers.[176] For example, the Commission has utilized the unfair business practices prong to hold two retailers responsible for transmitting consumers' payment information without encryption.[177] As a result of the retailers' failure, the consumers' payment information was stolen and fraudulently used.[178] The Commission took action against both retailers for their failure to take reasonable security measures.[179] When the Commission is deciding whether to take action against a company under this prong, it evaluates what was expected of the company, the sensitivity of the compromised data, and the number of different records the company has in its possession.[180] Practically, the Commission engages in a sliding-scale-type analysis: "[t]he larger the volume of and the more sensitive the consumer data that a company collects, the more detailed and sophisticated the security measures should be . . . ."[181] Multiple companies have attempted to challenge the Commission's authority under this prong, but the two significant challenges to the Commission's authority have faltered.[182]

III. ANALYSIS

Currently there is no singular regulatory scheme or law that attempts to regulate the wild wild west that is data security.[183] As discussed above, some states have enacted consumer protection laws designed to protect consumers after a breach occurred.[184] Additionally, the Federal Trade Commission has taken

174 *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 152 (2008).

175 15 U.S.C. § 45(n) (2018).

176 Solove & Hartzog, *supra* note 153, at 639.

177 Moncada, *supra* note 162, at 920.

178 *Id.*

179 *Id.*

180 Moncada, *supra* note 162 at 920–21.

181 *Id.*

182 *Id.*

183 *See supra* Part II.

184 *See supra* Part II.

an active role in after-the-fact regulation for data breaches.[185] However, state and Federal Trade Commission action fails to directly address and regulate the existing weaknesses with data protection and identity authentication, even though their action could potentially reduce the impact of the significant and increasingly frequent data breaches that each and every organization experiences.[186]

Section III.A. argues that Congress should act and address the underlying weaknesses in the identity authentication scheme. This can be effectuated by following the example of other nations that have achieved similar milestones, such as Canada.[187] This would be a significant shift from the current methodology of how organizations verify a consumer's identity. However, the shift would ultimately prove to be a worthwhile effort because consumer protection would be increased and fraudulent activity as a result from data breaches would ultimately be reduced. Next, Section III.B. will argue that consumers are currently ill informed as to what degree their information is collected by organizations and how the organizations utilize the information that is collected. The proposed solution to this issue is that Congress, or even the individual states, should enact legislation requiring organizations that collect personally identifiable information to clearly identify the data that they collect and explain how the data is utilized. Finally, Section III.C. will argue that Congress should directly empower the Federal Trade Commission to proactively enforce data security standards before data breaches occur. One avenue this could be accomplished through is the adoption of the Payment Card Industry Data Security Standards as a Federal Trade Commission regulation.[188]

A. The Social Security Number is an Ineffective Means of Authenticating a Consumer's Identity and Must Be Reformed

From the beginning, the social security number was never meant to serve the purpose that it currently serves: an end-all-be-all identification number.[189] Over time, organizations recognized that each citizen possessed a number that could serve as a unique individual identification and authentication method.[190] While it was initially convenient for companies to collect this information, the

185 *See supra* Section II.C.

186 *See supra* Section II.C.

187 Fraser, *supra* note 57, at 1; *see supra* Section II.A.

188 *See supra* Section II.A.

189 *Use and Misuse of Social Security Numbers: Hearing Before the Subcomm. on Soc. Sec. of the Comm. on Ways and Means*, 108th Cong. 11 (2003) (statement of Barbara D. Bovbjerg, Director, Education, Workforce, and Income Security Issues, U.S. General Accounting Office).

190 *Id.* at 8 (statement of Chairman Shaw).

explosion in the collection of data has had unintended consequences and wide-ranging impacts.[191] Further, the use of the social security number also has its own inherent deficiencies.

First, the social security number can be an ineffective means of identifying an individual because, for the first 75 years of issuing social security numbers, the numbers were not randomized.[192] Instead, the individual applying for the social security card received their number based upon their geographic location and year of birth.[193] This hampered the system for a few different reasons. First, the lack of randomization compromised the integrity of the social security number.[194] For example, armed with the correct information, an individual could accurately guess someone else's social security number because of the sequential number progression.[195] This discovery and inherent defect drastically compromises the security of the social security number.[196] In response, the Social Security Administration enacted a randomization process that was put in place on June 25, 2011, to "protect the integrity" of the social security number.[197] Although the Social Security Administration did take proper steps to remedy this defect, there remains a significant number of active social security numbers that can be guessed with the proper information.[198] Therefore, the social security number alone is an ineffective means of identifying individuals.

Next, your social security number is inherently difficult to have changed; so much so that the Social Security Administration only issued 274 new social security numbers in 2015.[199] In order to have a social security number changed,

---

191 *See, e.g.*, LoPucki, *supra* note 48, at 95–100 (2001) (discussing the implications of utilizing the social security card to verify the identity of individuals for common transactions such as retail credit accounts).

192 *Social Security Number Randomization*, SOC. SECURITY ADMIN., https://www.ssa.gov/employer/randomization.html (last visited Sept. 20, 2018).

193 Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SECURITY BULL. 2 (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

194 *See id.*

195 *Social Security Numbers are Easy to Guess*, AM. ASS'N FOR THE ADVANCEMENT OF SCI., (July 6, 2009), http://www.sciencemag.org/news/2009/07/social-security-numbers-are-easy-guess (discussing a study conducted by Carnegie Mellon University researchers who were able to accurately predict the Social Security numbers of individuals born after 1989).

196 *Id.* (finding that "a computer-savvy attacker could simultaneously test numbers on credit applications easily accessible online and harvest some 47 numbers per minute").

197 *Social Security Number Randomization*, *supra* note 192.

198 *Id.*

199 Dan Turkel, *Why It's Surprisingly Hard to Get a New Social Security Number if Yours Gets Stolen by Hackers*, BUS. INSIDER (Mar. 3, 2016, 3:51 PM), http://www.businessinsider.com/getting-new-social-security-number-2016-3.

the applicant must meet one of five requirements set out by the Social Security Administration.[200] Further, simply because an individual may meet one of those five requirements does not necessarily mean that the individual will be issued a new number.[201] By no means is changing your social security number a clear path to a fresh start either because many organizations may retain your old number or link the new and old numbers within their internal records.[202] Therefore, the fact that we are currently utilizing a virtually immutable number that is frequently stolen as the key to many transactions is a major weakness of the social security number. [203]

Third, the social security number is vastly overused by organizations that may not and often do not adequately protect the information.[204] What began as a method for citizens to obtain government benefits eventually morphed in to an identification number to which each and every business wanted access.[205] Among multiple motivations, businesses were motivated by the fact that they could establish accounting systems without investing in the development of their own identification numbers.[206] At the current time, this system has reached a point where businesses may refuse to provide their service to a consumer who does not provide their social security number.[207] Some examples of organizations that oddly require social security numbers include many public utility

---

200 *Can I Change My Social Security Number?*, SOC. SECURITY ADMIN. (last modified May 19, 2018), https://faq.ssa.gov/en-us/Topic/article/KA-02220 (stating that the requirements are (1) Sequential numbers assigned to members of the same family are causing problems; (2) More than one person is assigned or using the same number; (3) A victim of identity theft continues to be disadvantaged by using the original number; (4) There is a situation of harassment, abuse or life endangerment; or (5) An individual has religious or cultural objections to certain numbers or digits in the original number).

201 Turkel, *supra* note 199 (quoting a Social Security Administration spokesperson: "It is against our policy, the public's interest, and the integrity of our enumeration processes to assign new SSNs simply upon request or out of a concern there may potentially be a future problem[.]").

202 *Id.*

203 *See supra* Section II.A.

204 Jesse Emspak, *Why Overusing Social Security Number Is Risky*, NBC NEWS (July 8, 2011, 8:15 PM), http://www.nbcnews.com/id/43691269/ns/technology_and_science-security/t/why-overusing-social-security-number-risky/.

205 *Id.*

206 *Id.*

207 *Id.*

companies,[208] college student identification,[209] and cell phone companies.[210] Additionally, the overuse of the social security number led some federal, state, and local agencies to include social security numbers in public records.[211]

Given these weaknesses, among others, it is clear that the social security number has grown to purposes beyond what it was designed for and needs to be replaced or reimagined. A variety of different methods have been proposed to replace the social security number, but there can be no one-size-fits-all approach.[212] One potential solution could be sourced from Canada, which has recently addressed a similar issue with its social security number equivalent.[213] In Canada, the government recognized the issues with having a singular national identification number and enacted a sweeping privacy reform act.[214] A key feature of this act involved removing a company's ability to require a social insurance number before providing credit or other services.[215] However, this change has not exactly brought the results the Canadian government envisioned, as identity theft has gradually increased since the law's passage.[216]

Therefore, a more apt solution appears to be enacting a national multi-factor method for authentication.[217] In fact, the current administration is considering following this route, but it has not identified a likely multi-factor

---

[208] *Utility Services*, FED. TRADE COMMISSION (Aug. 2012), https://www.consumer.ftc.gov/articles/0220-utility-services.

[209] Farai Chideya, *The Way We Use Social Security Numbers Is Absurd*, FIVETHIRTYEIGHT (Oct. 15, 2015, 7:00 AM), https://fivethirtyeight.com/features/the-way-we-use-social-security-numbers-is-absurd/.

[210] Michael Huffington, *Why Does AT&T Need My Social Security Number to Connect My iPhone?*, HUFFPOST (Nov. 17, 2011), https://www.huffingtonpost.com/michael-huffington/why-does-att-need-my-soci_b_64526.html.

[211] *Use and Misuse of Social Security Numbers*, *supra* note 189, at 8 (statement of Chairman Shaw) (discussing efforts to address the disclosure of social security numbers in public records, but acknowledging that the disclosure will continue to be an issue for the time being).

[212] Lily Hay Newman, *Replacing Social Security Numbers Won't Be Easy, but It's Worth It*, WIRED (Oct. 13, 2017, 7:00 AM), https://www.wired.com/story/social-security-number-replacement.

[213] *See supra* notes 57–60 and accompanying text.

[214] Fraser, *supra* note 57, at 1 (discussing the adoption and application of the new privacy law).

[215] *Id.*

[216] *See* Justina Deardoff & Katherine Huitmea, *Identity Theft and Fraud Are on the Rise in Canada*, CALGARY J. (Feb. 10, 2015), https://www.calgaryjournal.ca/index.php/news/2633-identity-theft-and-fraud-are-on-the-rise-in-canada.

[217] Multi-factor authentication involves presenting two different pieces of evidence to verify your identity when accessing an account or a service. *See Back to Basics: Multi-factor Authentication (MFA)*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication (last updated Nov. 22, 2016).

authentication method.[218] One promising solution can be modeled after Estonia's system. In Estonia, each citizen is provided with a card that contains a unique physical chip and code that, when combined with the citizen's PIN and information on the organization's side, securely authenticates and authorizes the transaction.[219] No matter how the social security card is replaced, the effort to enact a bill authorizing the replacement will face significant pushback. Perhaps the most ardent opponents will be major industry players, like banks and credit reporting agencies. Their pushback will not be without merit because a new system may require significant financial outlay as the system is adopted. However, as the new system matures, banks and credit reporting agencies will see their financial losses due to fraud drop significantly.

B. Privacy Policies are Exceedingly Difficult for the Average Consumer to Decipher and Updates Must be Enacted for Uniform Disclosure of Information

With virtually every website one visits on the internet, the user is almost guaranteed to encounter a privacy policy. Some websites have an applicable privacy policy simply for website visitors,[220] and some websites have a separate privacy policy for users with accounts.[221] Unknown to many consumers, these policies often permit the companies to utilize the consumer's information in a variety of ways because the company is the ultimate arbiter of the policy's content.[222] Therefore, it is imperative that the form of privacy policies are standardized and consumers are properly educated about the information

---

[218] Kari Paul, *Trump Administration Wants to Replace Social Security Numbers with Something Less Vulnerable*, MARKETWATCH (Oct. 4, 2017, 7:45 AM), https://www.marketwatch.com/story/social-security-numbers-are-80-years-old-heres-how-america-could-replace-them-2017-09-15.

[219] *e-identity*, E-ESTONIA, https://e-estonia.com/solutions/e-identity/id-card (last visited Oct. 27, 2018); *Identity Documents*, EST. POLICE AND BORDER GUARD BOARD (Sept. 30, 2018) https://www2.politsei.ee/en/teenused/isikut-toendavad-dokumendid/.

[220] *See, e.g.*, *Privacy Policy*, WARNER BROS., https://www.warnerbros.com/privacy-center-wb-privacy-policy#collectinfo (last updated Dec. 8, 2017) ("Information may be collected as described below and through the use of cookies, web beacons, pixels, and other similar technologies by us or by other companies on our behalf."); *Walmart Privacy Policy*, WAL-MART, https://corporate.walmart.com/privacy-security/walmart-privacy-policy (last updated Nov. 2017) ("We collect two types of information . . . . This also includes information you provide us through technology, such as through a cookie placed on your computer when you visit our websites.").

[221] *See Privacy Policy*, APPLE, https://www.apple.com/legal/privacy/en-ww/ (last updated May 22, 2018); *Privacy Policy*, GOOGLE, https://www.google.com/policies/privacy/ (last updated May 25, 2018).

[222] *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 597 (2007).

companies are collecting and how that information is used. Without empowering consumers with this information, the data breaches companies and websites continue to experience will continue to present danger to unaware consumers.

Currently, the FTC takes the approach that companies should be freely permitted to determine how to respond to privacy challenges.[223] This approach has led to different companies sharing multiple common deficiencies with privacy policies. For example, the average privacy policy requires a heightened level of reading ability that a majority of consumers do not possess.[224] By writing a privacy policy in a complicated manner companies can achieve two potential benefits. First, the complicated language and overall length can lead consumers to either not read the policy or skim the policy, potentially missing important details.[225] Second, with a complicated policy, a company could encourage consumers to disclose more information than is necessary.[226] For example, some companies include ambiguous terms in their policies that permit the unlimited use of the information that is collected.[227] Overall, the majority of consumers do not take the appropriate time to familiarize themselves with a website's privacy policy.[228] Without empowering consumers with easy to understand information about privacy policies, companies will continue to stretch the bounds of information that is collected, and the impact of data breaches will continue to be significant.

One potential solution follows a "nutrition label" approach.[229] This approach has not yet been widely adopted, but it is designed to increase a consumer's understanding of a privacy policy by encouraging a consumer to take a quick glance for understanding.[230] Congress or individual states should enact specific legislation designed to require or strongly encourage companies to adopt a form of this innovation. Furthermore, a legislative body has precedent for taking this approach. For example, as recently as 1999, Congress enacted heightened disclosure requirements for financial institutions through the Gramm-

---

223 Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L. J. 39, 43–44 (2015).

224 *Id.* at 46.

225 *See id.* at 47.

226 *Id.* at 46.

227 *Privacy Policy*, BLUE APRON, https://www.blueapron.com/pages/privacy (last updated Mar. 1, 2017) (permitting the company to "[c]arry out any other purpose for which the information was collected").

228 *See* Reidenberg et al., *supra* note 223, at 83.

229 PATRICK GAGE KELLEY ET AL., CARNEGIE MELLON UNIV., STANDARDIZING PRIVACY NOTICES: AN ONLINE STUDY OF THE NUTRITION LABEL APPROACH 1–2 (2010), https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab09014.pdf.

230 *See id.*

Leach-Bliley Act ("GLB Act").[231] In pertinent part, the GLB Act permitted the FTC to determine that financial institutions must inform their customers, with a "clear and conspicuous" written notice, of the financial institution's privacy policies.[232] The institutions are required to disclose what information is collected, how the financial institution uses the information, whether or not consumers can limit the use, and if the financial institution shares the information with third parties.[233] Financial institutions responded to this requirement by developing the common form information disclosure statements that the majority of financial institutions currently utilize.[234] Therefore, the adoption of the GLB Act serves as an important guide for a legislative body to follow in reforming the use of privacy policies.

By adopting a "clear and conspicuous" notice requirement for privacy policies, Congress or a state legislature would be undertaking a significant change and may face pushback from the business community. Therefore, it is important that a deliberate approach is taken. For example, potential legislation should first focus on requiring the most frequently websites to update their privacy policies to be "clear and conspicuous." After several years, the remaining websites will be responsible for updating their policies. By this point, commercially available services will exist to assist the smaller websites in this venture. Ideally, migration will occur over a three to five-year period.

Ultimately, the benefit of better informing consumers vastly outweighs the cost of requiring more from websites and businesses when it comes to privacy. First and foremost, consumers will easily be able to understand what types of personal information organizations keep about them. This will, in turn, lead to consumers making informed decisions to either use or not use the website or service. Once consumers know what information is being retained, they can request that companies either not collect their information or remove their information from the company's files. While this action will not directly lead to a decrease in the number of data breaches, the impact of data breaches will be reduced. The impact will be reduced because companies will be less likely to

231 15 U.S.C. §§ 6801–09 (2018).

232 15 U.S.C. § 6803.

233 FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT 7–8 (2002), https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

234 *See, e.g.*, *What Does Discover Bank Do with Your Personal Information?*, DISCOVER, https://www.discover.com/privacy-statement/credit-cards-privacy-policy.html (last updated Sept. 2018); *What Does American Express Do with Your Personal Information?*, AMERICAN EXPRESS, https://web.aexp-static.com/us/content/pdf/legal-disclosures/privacy-notices/Personal-Charge.pdf (last updated Apr. 2018).

retain significant amounts of personally identifiable information that are not directly relevant to their businesses.

C. Congress Should Empower the Federal Trade Commission to Adopt the Payment Card Industry Data Security Standards as a Regulatory Scheme to Ensure the Security of Consumer Financial Information

Currently, the FTC mainly focuses on conducting reactive investigation and enforcement actions against companies that have suffered data breaches or have caused losses to consumers.[235] The FTC's enforcement ability is rooted in an over one-hundred-year-old statute.[236] Under this statute, the FTC is permitted to investigate and take action against a company's unfair or deceptive data security practices.[237]

However, this form of regulation is ineffective for a few reasons. First, the FTC most often takes a reactive approach to data breaches.[238] This reactive approach means that a company with weak data security policies will go unmonitored until the company experiences a significant data breach, which then attracts the attention of the FTC. Thus, the potential impact of a company's weak data security policy is amplified, and consumers' personally identifiable information is placed at risk. Second, the ability of the FTC to investigate and sanction companies after a data breach, under the unfair practices prong, is not clear and has faced court challenges.[239] While the FTC has not lost a challenge to its powers under the unfair practices prong, it is unclear if a company will eventually succeed in a challenge.[240] Therefore, the FTC requires clear authority in this area.

Presently, the most active form of regulation comes from the Payment Card Industry Data Security Standards. Under these standards, companies that process transactions through the five major card payment networks must ensure adequate security.[241] Through this primarily contractual relationship, companies are subjected to announced audits by PCI as a requirement under the standards.[242] However, some companies merely view the audit as a hoop to jump through on a yearly basis.[243] While the standards aim to encourage compliance through fines

235 *Privacy & Data Security Update*, *supra* note 155, at 1.

236 Federal Trade Commission Act of 1914 § 5, 15 U.S.C. § 45 (2018).

237 Frechette, *supra* note 158, at 1403.

238 *See* Moncada, *supra* note 162, at 912–14.

239 *See id.* at 921–24.

240 *Id.* at 923–24.

241 PCI SEC. STANDARDS COUNCIL, *supra* note 116.

242 Weinstein, *supra* note 121, at 927–28.

243 *Id.* at 929.

and private sanctions, now is the appropriate time for Congress to take action and empower the FTC to proactively ensure the security of consumers' information.

To take action, Congress should amend the Federal Trade Commission Act to explicitly allow the Commission to take a proactive approach with payment card information data security. Under this amendment, discretion should be left to the Commission to enact necessary rules. The Commission should then adopt the PCI-DSS framework as a base level regulatory framework, with necessary improvements. For example, one improvement could strengthen the process of verifying compliance with the standards and identify potential alternative sanctions beyond fines. Overall, this proposal would face pushback from industry for a variety of reasons. As with most increased regulation, the industry would argue that companies' financial burdens from the investment in new systems would be too great.

But the benefits to consumers outweigh the burdens placed on the companies. For example, approximately $178 trillion is transmitted through non-cash payments each year.[244] Therefore, there is a real and significant financial interest for both the government and companies to adopt a stringent set of standards to secure consumers' financial information. By adopting the PCI-DSS standards, companies would ultimately end up spending less money to cover losses due to fraud. Furthermore, consumer confidence could increase, and the economy could grow as a result of electronic payments being more secure. More specifically, rather than being considered a one-and-done checklist, the Commission would be able to ensure that the proper level of attention is given to the regulations and that the impact for noncompliance is significant enough to deter noncompliance. Overall, the benefits of these regulations would outweigh the harms to the companies and would result in a more consumer-friendly environment.

IV. CONCLUSION

Every day, consumers are providing a significant amount of personally identifiable information and financial information to companies. Each time a consumer swipes his or her credit card, signs on to a website, or searches the internet, a piece of information is generated about the consumer. While the different pieces of information alone may not be impactful if disclosed, the total volume of information generated each day makes all information a valuable target for attackers. Attackers continually attempt to infiltrate computer systems and are often successful. Therefore, it is imperative that steps are taken to curb the risk of providing the personally identifiable information consumers are required to provide in virtually every transaction. The best long-term solutions

244 *The Federal Reserve Payments Study*, *supra* note 34, at 2.

for consumers, the government, and businesses would be to implement a national multi-factor method for authentication instead of using social security numbers, to require companies to provide users with clear privacy policies, and to allow the Federal Trade Commission to be proactive with securing payment card information data.

Jacob Holden[*]

[*] J.D., West Virginia University College of Law, 2018; B.S. Criminal Justice, West Liberty University, 2014. The Author would like to thank the members of the *West Virginia Law Review* for their hard work and dedication in preparing this Note for the Volume 121 publication. This note would not have been possible without the continual support of the Author's friends and family, and for that he will always be grateful.