Cite as Smith & Mulrain, 9 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2018)

Equi-failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform

McKay Smith[*] & Garrett Mulrain[**]

[*] McKay Smith is an Attorney with the U.S. Department of Justice, National Security Division. He is also an Adjunct Professor at the George Washington University Law School and the George Mason University School of Law where he teaches courses on government oversight and internal investigations. Mr. Smith served as a Senate Fellow for John McCain on the Senate Armed Services Committee. Prior to joining the Department of Justice, Mr. Smith also worked as a Senior Inspector with the Department of Homeland Security, Office of Inspector General. He served in multiple capacities within that office, including as an Attorney and as the Acting Intelligence Operations Specialist. Mr. Smith earned an LL.M., with distinction, from the Georgetown University Law Center, a J.D. from William and Mary Law School, and a B.A. from the College of William and Mary. The views expressed in this article are those of the author and do not necessarily represent the views of the Department of Justice, the U.S. Senate, the Department of Homeland Security, or the United States.

[**] Garrett Mulrain is a Law Clerk with the American Bar Association Standing Committee on Law & National Security, which is charged with maintaining a diverse program of scholarship, conferences, working groups, and publications dedicated purely to law and national security-related issues. Specifically, Mr. Mulrain oversees a portfolio that includes cybersecurity, cyberwarfare, the Intelligence Community, the Foreign Intelligence Surveillance Act, Guantanamo Bay litigation, and national security legislation. Prior to his clerkship, Mr. Mulrain worked with the Civil Rights Division of the Department of Homeland Security's Transportation Security Administration, as well as with the International Criminal Tribunal for the Former Yugoslavia in the Hague. He has represented Human Rights Watch as a European Union policy intern before the European Parliament in Brussels, Belgium and has also clerked for the Egyptian-American Rule of Law Association. Mr. Mulrain earned an LL.M. in National Security & U.S. Foreign Relations Law, with highest honors, from the George Washington University Law School, and an LL.B. from University College Cork, Ireland. He also graduated from the Erasmus Mundus program while studying at the University of Copenhagen in Denmark.

TABLE OF CONTENTS

Table of Contents	2
I. Introduction	3
II. The Equifax Hack	7
III. Detailed Timeline of Events	12
IV. National Security Implications	15
V. Overview of the Current Legal Regime	22
A. The Financial Services Modernization Act	25
B. The Fair Credit Reporting Act	27
C. The Federal Trade Commission Act	29
VI. Recommendations for Reform	31
A. Recommendation #1 - Establish a New Bipartisan Commission	32
B. Recommendation #2 - Create a New Information Security Agency	35
C. Recommendation #3 - Enhance Current Information Security Oversight	38
D. Recommendation #4 - Implement a Minimum Standard of Cyber Care	40
E. Recommendation #5 - Design a Cyber Hygiene Public Awareness Campaign	44
F. Recommendation #6 - Utilize Third-Party Penetration Testers	45
G. Recommendation #7 - Employ Chief Information Security Officers	47
VII. Conclusion	49
Appendix I - Detailed Timeline of Events	51
Appendix II - Comparison Chart of FTC vs. CFPB vs. Information Security Agency	52
Appendix III - Proposed Organizational Chart for the Information Security Agency	53

> *"It's like the guards at Fort Knox forgot to lock the doors and failed to notice the thieves were emptying the vaults.... How does this happen when so much is at stake? I don't think we can pass a law that, excuse me for saying this, fixes stupid. I can't fix stupid."*[1]
>
> Representative Greg Walden, Oregon

I. INTRODUCTION

Throughout 2017, Americans felt powerless to protect themselves, and their most private information, from malicious cyberattacks and data breaches. In March 2017, WikiLeaks published a trove of documents that allegedly revealed sophisticated software tools used by the Central Intelligence Agency to spy on computers, smartphones, and internet-connected televisions.[2] Just two months later, the WannaCry ransomware attack crippled computers in more than 150 countries, including the United States, and shut down hospitals across Europe.[3] Corporate America was not immune from cyber intrusions as Yahoo publicly disclosed in October 2017 that the accounts of all of its customers, 3 billion in total, had been compromised

[1] *Oversight of the Equifax Data Breach: Answers for Consumers*: *Hearing Before the H. Subcomm. on Digital Commerce and Consumer Protection, Comm. on Energy and Commerce*, 115th Cong., 1st Sess. (2017) [hereinafter *Oversight of the Equifax Data Breach Hearing*] (preliminary transcript) (statement of Rep. Greg Walden, Chairman, Comm. on Energy and Commerce) (addressing the Equifax data breach and the factors that led to the theft of the personally identifying information of over 143 million Americans, in particular Equifax's failure to apply a critical software patch in March of 2017).

[2] Scott Shane, Matthew Rosenberg, & Andrew Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html; Jose Pagliery, *WikiLeaks Claims to Reveal How CIA Hacks TVs and Phones All Over the World*, CNN: TECH (Mar. 8, 2017), http://money.cnn.com/2017/03/07/technology/wikileaks-cia-hacking/index.html.

[3] Elizabeth Dwoskin & Karla Adam, *More Than 150 Countries Affected by Massive Cyberattack, Europol Says*, WASH. POST (May 14, 2017), https://www.washingtonpost.com/business/economy/more-than-150-countries-affected-by-massive-cyberattack-europol-says/2017/05/14/5091465e-3899-11e7-9e48-c4f199710b69_story.html; *Massive Ransomware Infection Hits Computers in 99 Countries*, BBC: TECHNOLOGY (May 13, 2017), http://www.bbc.com/news/technology-39901382.

years earlier.[4] Moreover, in November 2017, Uber shocked consumers when it admitted that it failed to notify victims for over a year after paying $100,000 to hackers who had stolen data on 57 million users and drivers.[5] In terms of potential damage to national security, however, all of these events pale in comparison to last year's devastating hack of Equifax, Inc.

Equifax is one of the nation's largest credit reporting agencies,[6] and there is little question that it recently suffered one of the most significant data breaches in U.S. history.[7] The Equifax hack resulted in the loss of vital information - names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers - for 143 million people, impacting nearly half the U.S. population.[8] Because of Equifax's failure to apply a critical software patch,[9] average consumers will now be forced to actively monitor their financial

[4] Matt O'Brien, *Yahoo: 3 Billion Accounts Breached in 2013. Yes, 3 Billion*, AP NEWS, (Oct. 3, 2017), https://www.apnews.com/06a555ad1c19486ea49f6b5b80206847.

[5] Mike Isaac, Katie Benner, & Sheera Frankel, *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html; Julia Wong, *Uber Concealed Massive Hack That Exposed Data of 57M Users and Drivers*, THE GUARDIAN: TECHNOLOGY (Nov. 22, 2017), https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

[6] *See* ABOUT EQUIFAX, COMPANY PROFILE, https://www.equifax.com/about-equifax/company-profile. Equifax, Inc. describes itself as a "global information solutions company that uses unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions." In essence, credit reporting agencies are companies that help businesses assess the creditworthiness of individual consumers, by compiling and selling credit data about that consumer's financial history. Equifax is one of the largest, alongside Experian and TransUnion, and its 10,000 employees are located in over 24 countries. *See also* Jeffrey Bils, *Fighting Unfair Credit Reports: A Proposal to Give Consumers More Power to Enforce the Fair Credit Reporting Act*, 61 UCLA L. REV. DISC. 226, 229 (2013) ("The effort to track the credit histories of 200 million American consumers is a multibillion-dollar industry dominated by three companies: Experian, TransUnion, and Equifax.").

[7] Allen St. John, *Equifax Data Breach: What Consumers Need to Know*, CONSUMER REPORTS (Sept. 21, 2017), https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/ (describing the Equifax breach as one of the most significant data breaches in recent history).

[8] *Id.*; Alyssa Newcomb, *Massive Equifax Data Breach Could Affect Half of the U.S. Population*, NBC NEWS (Sept. 10, 2017), https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686 (explaining the vast implications of the Equifax breach as it relates to American consumers); Brian Womack, Jordan Robertson, & Michael Riley, *Equifax's Historic Hack May Have Exposed Almost Half of U.S.*, BLOOMBERG (Sept. 8, 2017), https://www.bloomberg.com/news/articles/2017-09-08/equifax-s-historic-hack-may-have-exposed-almost-half-of-u-s (referring to Equifax's "historic hack" of nearly half the U.S. population).

[9] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 20; *see also* David Shepardson, *Equifax Failed to Patch Security Vulnerability in March: Former CEO*, REUTERS (Sept. 8, 2017), https://www.reuters.com/article/us-equifax-breach/equifax-failed-to-patch-security-vulnerability-in-march-former-ceo-idUSKCN1C71VY.

information for decades.[10] Moreover, our national security is at risk, with unprecedented potential for future cyberattacks, cybercrime, foreign financial blackmail, and other hostile nation-state activities.[11]

America's lawmakers initially approached the Equifax hack with bipartisan anger, peppering Richard Smith, the former Chief Executive Officer, with questions about software vulnerabilities, security practices, and consumer remediation.[12] Several Members also proposed legislation meant to impose additional regulations on Equifax, and the larger credit reporting industry.[13] In the ensuing weeks, however, "the aftermath of the breach played out like a familiar script … white-hot, bipartisan outrage, followed by hearings and a flurry of proposals that went nowhere."[14] In the halls of the Capitol, lawmakers could be heard muttering a familiar refrain,

[10] Kelli B. Grant, *How to Protect Yourself After the Equifax Breach: Assume You're Affected*, CNBC (Sept. 8, 2017), https://www.cnbc.com/2017/09/08/how-to-protect-yourself-after-the-equifax-data-breach.html (quoting Neal Creighton, the chief executive of the security firm Countertrack, who asserts that the daily life of the average consumer has now changed, and that "the first assumption a consumer should make is that they are affected*"); see generally* Lauren L. Sullins, *"Phishing" For a Solution: Domestic and International Approaches to Decreasing Online Identity Theft*, 20 EMORY INT'L L. REV. 397 (2006) (noting the danger of "phishing" and how little personal data is required to steal consumers identities).

[11] *See generally* John P. Carlin, *Detect, Disrupt, Deter: A Whole-Of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391 (2016) (describing the myriad cyber threats facing our country, including traditional nation states, as well as non-state, terrorist actors); Mark D. Young, *United States Government Cybersecurity Relationships*, 8 I/S: J. L. & POL'Y FOR INFO. SOC'Y 281 (2012) (discussing ways in which to better design, build, manage, and defend the information infrastructure on which American society depends); RICHARD A. CLARKE & ROBERT K. KNAKE, *Cyber War: The Next Threat To National Security and What To Do About It* (HarperCollins Publishers 2010) (analyzing the cyber-threat posed by hostile nation state activity, including an assessment of "cyber-warriors").

[12] *See generally Oversight of the Equifax Data Breach Hearing*, *supra* note 1; *see also* Hamza Shaban, *'This is a Travesty': Lawmakers Grill Former Equifax Chief Executive on Breach Response*, WASH. POST (Oct. 2, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/what-to-expect-from-equifaxs-back-to-back-hearings-on-capitol-hill-this-week/; Seth Fiegerman & Donna Borak, *Former Equifax CEO Testifies Before Congress*, CNN: Money (Oct. 3, 2017), http://money.cnn.com/2017/10/03/news/companies/equifax-ceo-congress/index.html.

[13] *See* Ali Breland, *Lawmakers Push Credit Report Legislation After Equifax Breach*, THE HILL (Sept. 11, 2017), http://thehill.com/policy/technology/350104-lawmakers-introduce-credit-report-legislation-after-equifax-breach (summarizing various legislative proposals, including those put forward by Senators Brian Schatz, Elizabeth Warren, and Claire McCaskill); Charlie Mitchell, *Equifax Breach Puts New Energy Into Data Legislation*, WASH. EXAMINER (Oct. 30, 2017) http://www.washingtonexaminer.com/equifax-breach-puts-new-energy-into-data-legislation/article/2638866 (discussing legislative initiatives put forward by Representatives Jeb Hensarling, Patrick McHenry, and Blaine Luetkemeyer).

[14] Martin Matishak, *After Equifax Breach, Anger but No Action in Congress*, POLITICO (Jan. 1, 2018, 7:39 AM), https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631.

"Wait until next year."[15] Notably, Equifax had aggressively lobbied Congress in the year prior, spending $1.1 million to counter legislation intended to improve the industry's data security and victim notification procedures.[16]

Americans still deserve answers. Moreover, American consumers deserve an effective and critical solution that goes beyond mere legislation to create a whole-of-government approach to cybersecurity.[17] The Equifax hack should be viewed as a triggering event for worthwhile government reform and increased public-private cooperation, creating a model that is both scalable and adaptable to multiple industries. Improvements within the credit reporting industry therefore represent an important first step to increased data security. They signify the U.S. government's renewed commitment to protecting its private corporations, and the data of private citizens, from malicious foreign adversaries. After all, while the cyber threat landscape of 2017 certainly seems daunting in retrospect, who knows what dangers the future holds.[18]

This article begins with a detailed account and timeline of the Equifax data breach, focusing on the national security implications of this widespread and devastating attack on the

[15] *Id.* (referencing Senator John Thune's comment that as much as he favors "an effective and coordinated approach on data security issues across industries, the reality is that our legislative progress has been much more incremental this year"); *see also* Kevin Freking, *After Equifax Breach, Congress Unlikely to Pass New Rules to Protect Consumer Data*, PBS (Sept. 22, 2017, 10:57 AM), https://www.pbs.org/newshour/nation/equifax-breach-congress-unlikely-pass-new-rules-protect-consumer-data.

[16] Michael Rapoport & AnnaMaria Andriotis, *Equifax Lobbied for Easier Regulation Before Data Breach*, WALL ST. J. (Sept. 11, 2017, 10:39 PM), https://www.wsj.com/articles/equifax-lobbied-for-easier-regulation-before-data-breach-1505169330?mod=e2tw ("Equifax Inc. was lobbying lawmakers and federal agencies to ease up on regulation of credit-reporting companies in the months before its massive data breach."); Renae Merle & Hamza Shaban, *Before the Breach, Equifax Sought to Limit Exposure to Lawsuits*, WASH. POST: BUSINESS (Sept. 19, 2017), https://www.washingtonpost.com/business/economy/before-the-breach-equifax-sought-to-limit-exposure-to-lawsuits/2017/09/19/8e6c8020-9d47-11e7-9083-fbfddf6804c2_story.html?utm_term=.27b266c8a71a ("The company's spending on lobbying peaked at $1.1 million last year, and Equifax has spent $500,000 already this year.").

[17] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA (Dec. 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; *see also* Carlin, *supra* note 11, at 394, 430 (noting that cyber threats demand a "whole-of-government" response and increased public-private partnerships).

[18] Matishak, *supra* note 14 ("With no sign that mammoth data breaches like the one at Equifax are abating, the situation is only growing more dire, according to cyberspecialists.").

American consumer economy. Recognizing that current regulation of the credit-reporting industry is inadequate,[19] the following argument also provides a detailed analysis of government oversight efforts. Finally, in an attempt to remedy existing deficiencies, this article contains a novel and creative proposal for reform which includes measures designed to turn our current reactive stance on corporate security into an active model of cyber defense.

II. THE EQUIFAX HACK

On September 7, 2017, Equifax, one of the largest consumer-credit reporting agencies in the world, publicly announced that its consumer information had been compromised as a result of a "cybersecurity incident."[20] This "incident" resulted in the loss of the personally identifiable information (PII)[21] of 143 million American consumers, or nearly 45 percent of the U.S. population.[22] The number would later be updated to 145.5 million Americans.[23]

[19] David D. Schein & James D. Phillips, *Holding Credit Reporting Agencies Accountable: How the Financial Crisis May be Contributing to Improving Accuracy in Credit Reporting*, 24 LOY. CONSUMER L. REV. 329 (2012) (explaining the breakdown between different judicial circuits in their interpretation of the Fair Credit Reporting Act, and how this adds to lack of oversight for a changing industry).

[20] EQUIFAX, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[21] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), DEP'T OF COMMERCE, SPECIAL PUBLICATION 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010) *citing* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-536-1, PRIVACY: ALTERNATIVES EXIST FOR ENHANCING PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (2008). For the purposes of this discussion, and in the context of a data breach, this article relies on the broad technical definition of PII included in the NIST's Guide to Protecting PII, which defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." This definition is GAO's expression of an amalgam of the definitions of PII from OMB Memorandums 07-16 and 06-19. For the federal government's legal framework for protecting PII please see The Privacy Act of 1974 and The E-Government Act of 2002.

[22] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 4 (statement of Rep. Bob Latta, Member, Comm. on Energy and Commerce).

[23] Spencer Kimball & Liz Moyer, *Equifax Data Breach May Affect 2.5 Million More Consumers than Originally Stated*, CNBC (Oct. 2, 2017), https://www.cnbc.com/2017/10/02/equifax-2-point-5-million-more-consumers-may-be-affected-by-data-breach-than-originally-stated.html.

The actual breach had occurred months earlier, from May 2017 to July 2017,[24] during which time the hackers gained access to the names, Social Security numbers, birth dates, addresses, and driver's license numbers of American consumers.[25] Moreover, the credit card information of nearly 209,000 people was compromised, as well as PII from credit dispute documents for an additional 182,000 victims.[26] The impact of the breach was not strictly national, as hackers were able to obtain information on citizens of the United Kingdom and Canada as well.[27] This led the Executive Director of the World Privacy Group, a nonprofit dedicated to research on information and data privacy, to issue an ominous warning – "This is about as bad as it gets…. If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent."[28]

Ironically, many individuals compromised by the Equifax hack had never even interacted with the company.[29] Due to the nature of the credit reporting industry, Equifax's business model relies on collecting, selling, and *securing* the financial information of millions of Americans.[30] In

[24] EQUIFAX, *2017 Cybersecurity Incident & Important Consumer Information*, https://www.equifaxsecurity2017.com/consumer-notice/; *see also Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 20 (prepared testimony and statement of Richard Smith, former Chief Executive Officer, Equifax).
[25] St. John, *supra* note 7.
[26] EQUIFAX, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, *supra* note 20.
[27] John Leyden, *UK Financial Regulator Confirms it is Probing Equifax Mega-Breach*, THE REGISTER (Oct. 24, 2017), https://www.theregister.co.uk/2017/10/24/equifax_fca_probe/; Seena Gressin, *The Equifax Data Breach: What to Do*, Federal Trade Commission (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do. Equifax, a U.S.-based company, originally reported that the breach resulted in the compromise of information on 400,000 British citizens. That number was adjusted to almost 700,000. The Financial Conduct Authority, the primary financial regulatory agency in the United Kingdom, is investigating the crime and could require a fine or even the revocation of Equifax's right to operate in Britain.
[28] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.
[29] *Id.*
[30] CONSUMER FINANCIAL PROTECTION BUREAU, WHAT IS A CREDIT REPORTING COMPANY? (2017), https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-reporting-company-en-1251/ ("Credit reporting companies can gather information from many sources including thousands of lenders across the country; public records, such as bankruptcies, garnishments, liens, and other judgments; and collections agencies, which provide information on delinquent accounts.").

fact, much of the information does not result from activities or requests of the actual consumers themselves.[31] It is instead generated as a result of routine credit checks of individuals living or working in the United States.[32] Unfortunately, this type of information is a prime target for hackers.[33] If malicious actors are able to break through the security defenses of one of these credit reporting agencies, they instantly have access to a cyber warehouse of data, a robust collection of consumer information otherwise unavailable in one central location.[34]

The Department of Homeland Security alerted Equifax officials on March 8, 2017 that they needed to fix a critical security vulnerability in their software.[35] Company officials disseminated the alert internally but failed to manually patch the application.[36] This single point of failure would prove to be catastrophic.[37]

Once the breach was made public through a nationwide press release, Equifax set up a website for consumers to determine if their PII had been compromised.[38] This solution had

[31] Bernard, et al., *supra* note 28.
[32] *Id.*; *see also* Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.
[33] *See* Jordan Robertson, *The Changes Coming to Credit Agencies Won't Stop Hackers*, BLOOMBERG (Mar. 9, 2015), https://www.bloomberg.com/news/articles/2015-03-09/the-changes-coming-to-credit-agencies-won-t-stop-hackers.
[34] *See Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 7-8 (statement of Rep. Janice Schakowsky, Member, Comm. on Energy and Commerce). In her statement, Rep. Schakowsky described the lack of oversight in the consumer industry. She stated, "145.5 million American victims as of yesterday. I would call it shocking, but is it really? We have these under-regulated, private, for-profit credit reporting agencies collecting detailed personal and financial information about American consumers. It is a treasure trove for hackers…. If you want to participate in today's modern economy, if you want to get a credit card, rent an apartment, or even get a job, often then a credit reporting agency may hold the key … once your information is compromised the damage is ongoing … hackers exploited a known vulnerability that was not yet patched."
[35] Tara Siegel Bernard & Stacy Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says,* N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html; COMPUTER EMERGENCY READINESS TEAM (CERT), AUTOMATED INDICATOR SHARING (AIS), https://www.us-cert.gov/ais. The alert given to Equifax was from a free program offered by the Department of Homeland Security, known as the Automated Indicator Sharing System. It allows information about potential threats and vulnerabilities to be shared between the public and private sector.
[36] Newman, *supra* note 32; *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 3 (prepared testimony and statement of Richard Smith, former Chief Executive Officer, Equifax).
[37] Bernard & Cowley, Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says, *supra* note 35.
[38] EQUIFAX, 2017 Cybersecurity Incident & Important Consumer Information, *supra* note 24; *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 20-21.

several shortcomings.[39] Consumers were understandably hesitant to enter additional personal information to see if their PII had been breached.[40] They worried that it would only compound the problem.[41] Equifax also recommended signing up for a one-year credit monitoring service called TrustedID.[42] Unfortunately, this free service required users to submit to mandatory arbitration.[43] In other words, anyone who used TrustedID would be forbidden to sue, join a class-action suit, or benefit from a class-action settlement.[44]

Moreover, the one-year protection plan fell far short of what was needed for aggrieved customers. This type of sensitive data will likely be bought and sold on the dark web for decades.[45] Adam Levin, chairman of the cybersecurity company CyberScout, underscored the problem when he stated, "This is a one-year solution for an eternal problem…. The collateral damage can be devastating, and when you are talking about Social Security numbers the only expiration date a Social Security number has is yours."[46] Paul Stephens, director of policy and

[39] *See, e.g.*, Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter To A Scam Site*, FORBES (Sept. 21, 2017), https://www.forbes.com/sites/janetwburns/2017/09/21/equifax-was-linking-potential-breach-victims-on-twitter-to-a-scam-site/#61ad2313288f; Maggie Astor, *Someone Made a Fake Equifax Site. Then Equifax Linked to It*, N.Y. TIMES (Sept. 20, 2017). The rollout of the Equifax security website was also met with controversy. Specifically, when Equifax launched the website, private web developer Nick Sweeting wanted to demonstrate how simple it would be to create an alternate website that mirrored its content. The new domain, www.securityequifax2017.com, was so convincing that Equifax tweeted the false link on several occasions.

[40] Brian Fung, *Equifax Finally Responds to Swirling Concerns Over Consumers' Legal Rights*, WASH. POST (Nov. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.6ee25c569709 ("Equifax's data breach site asks for your last name and the final six digits of your Social Security number. This is extremely unusual … that you must volunteer more of what would otherwise be private information…").

[41] *Id.*

[42] *Id.*

[43] *Id.*; *see also* Rep. John Conyers, et al., *Another Lesson from Equifax - We Must End the Predatory Consumer Practice of Forced Arbitration*, THE HILL (Oct. 4, 2017), http://thehill.com/blogs/congress-blog/judicial/353776-another-lesson-from-equifax-we-must-end-the-predatory-consumer.

[44] Fung, *supra* note 40.

[45] *See, e.g.*, Andy Greenberg, *Hacker Lexicon: What is the Dark Web?*, WIRED (Nov. 19, 2014), https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (providing a concise yet comprehensive overview of how the dark web works, and how it facilitates the sale of hacked consumer data).

[46] Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, N.Y. TIMES (Sept. 8, 2017), https://www.nytimes.com/2017/09/08/business/equifax.html.

advocacy at Privacy Rights Clearinghouse, was even more candid in his assessment.[47] He remarked that the effects of the hack will be felt for "essentially a hundred years, until everybody is dead that was exposed by this breach."[48]

Perhaps even more troubling, this was the third major cybersecurity breach of Equifax's systems in two years.[49] In 2016, hackers successfully stole critical W-2 tax and salary information from an Equifax website.[50] Earlier in 2017, an Equifax subsidiary known as TALX, which organizes payroll, tax, and human resource services for large corporations, was also breached.[51] There is one important distinction, however. After the most recent Equifax breach was discovered, but before it was disclosed to the general public, three senior executives sold approximately $1.8 million worth of their shares, causing the company's stock to plummet nearly 18 percent.[52]

Without additional legislation and a critical proposal for reform, consumers will be left to fend for themselves when it comes to protecting against data thieves and the fallout from this massive cyber breach.[53] The lasting consequences of the Equifax hack are still unknown, but a

[47] Laura Hautala, *Equifax Hack May Shake Up US Consumer Data Laws*, CNET: TECHNOLOGY (Oct. 20, 2014), https://www.cnet.com/news/equifax-hack-may-shake-up-consumer-data-laws/.
[48] *Id.*
[49] Tory Newmyer, *The Finance 202: Hard-Line Conservatives Endanger Wall Street Agenda*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/news/powerpost/paloma/the-finance-202/2017/09/08/the-finance-202-hard-line-conservatives-endanger-wall-street-agenda/59b1ac4830fb045176650bbb/?utm_term=.7a4c55cc24db.
[50] Bernard, et al., *supra* note 28.
[51] *Id.*; *see also* EQUIFAX, MANAGE MY WORKFORCE, https://www.equifax.com/business/manage-my-workforce; Brian Krebs, *Equifax Breach: Setting the Record Straight*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/equifax-breach-setting-the-record-straight/. The breach of TALX, which is now known as Equifax Workforce Solutions, was due to customers authenticating their payroll data by using a simple 4-digit personal identification number. According to Brian Krebs, this was a particular easy hack, as there just are not that many 4 digit PIN combinations.
[52] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.
[53] Yuki Noguchi, *After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips To Protect Your Data*, NPR (Sept. 14, 2017), https://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-

compromise of this type of data can lead directly to the misuse of medical histories, bank account information, and even employment information.[54] Moreover, this breach demonstrates that PII, and consumer data more generally, are a valuable commodity that must be protected.[55] These types of attacks cannot be written off merely as the malicious activity of a lone cybercriminal, intent on committing credit card fraud or identity theft.[56] Rather, the most devastating cyberattacks and data breaches are often perpetrated by adversarial nation states or their agents.[57]

III. DETAILED TIMELINE OF EVENTS

The timeline of events[58] surrounding the Equifax hack is discouraging, as it demonstrates the company's lack of appreciation for the seriousness of the breach, as well as data security practices writ large.[59] As described above, on March 7, 2017, the Department of Homeland Security discovered a critical security flaw in specific versions of web-application software

their-own ("When it comes to dealing with the aftermath of Equifax's massive data breach, it'll be up to consumers to be on guard against data thieves, experts say.").

[54] *See* Brigid Sweeney, *The Frightening New Frontier for Hackers: Your Medical Records*, CRAIN'S: CHICAGO BUSINESS (Apr. 8, 2017), http://www.chicagobusiness.com/article/20170408/ISSUE01/170409897/the-frightening-new-frontier-for-hackers-your-medical-records; *see also* Sullins, *supra* note 10. According to cybersecurity scholars, the hacking of medical information is more lucrative than most other types of information. While some hacks of personal information only include names and/or addresses, health records almost always include social security numbers and bank payment information. Furthermore, in an effort to provide better service, health records are increasingly going digital.

[55] *See* Carlin, *supra* note 11, at 405. John Carlin draws a strong link between personally identifiable information and national security threats. When private companies are charged with storing and collecting large amounts of data, they become prime targets for foreign nefarious purposes. The threat is sometimes discounted as identity-theft, yet the lack of public, and government, awareness on this issue creates a systemic and undeniable risk to the United States as a whole.

[56] *See generally* Kristin E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317 (2015); KRISTIN FINKLEA & CATHERINE A THEOHARY, CONG. RESEARCH SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT (2015).

[57] FINKLEA & THEOHARY, *supra* note 56, at 11.

[58] *See* Appendix I – *Detailed Timeline of Major Events* [hereinafter Appendix I].

[59] Newman, *supra* note 32 ("Capping a week of incompetence, failures, and general shady behavior in responding to its massive data breach … numerous doubts have surfaced about the organization's competence as a data steward.").

named "Apache Struts."[60] Most companies that used the software, including Equifax, were alerted to the flaw that very same day.[61] Nonetheless, Equifax reported that hackers first gained "unauthorized access" to their systems on May 13, 2017, sixty-seven days after they were notified of the patch.[62] Moreover, malicious actors were able to operate with impunity until July 29, 2017, when Equifax's security investigators first noticed suspicious network traffic on their online dispute portal.[63] It was at this stage that "the Security team investigated and blocked the suspicious traffic."[64] The hack itself was over, but Equifax's systems had been compromised for approximately seventy-seven days.[65]

On August 2, 2017, Equifax retained the law firm King & Spalding LLP.[66] They also hired the independent cybersecurity firm Mandiant,[67] which was charged with "conducting a privileged, comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted."[68] It took thirty-three more days, until September 4, 2017, for Mandiant to assemble a list of the 143 million victims.[69] During this period, on August 22, 2017, Equifax registered the domain name www.equifaxsecurity2017.com, which would ultimately be used for

[60] *Apache Patch Announcements General Availability*, APACHE (Mar. 7, 2017), https://struts.apache.org/announce.html#a20170307-2.
[61] EQUIFAX, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes (Sept. 15, 2017) https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832; *see also* Appendix I.
[62] MAJORITY STAFF OF H. COMM. ON ENERGY AND COMMERCE, 115th Cong., MAJORITY MEMORANDUM FOR OCTOBER 3, 2017, SUBCOMMITTEE ON DIGITAL COMMERCE AND CONSUMER PROTECTION HEARING (2017) [hereinafter *Timeline*] (including detailed outline prepared in anticipation of the hearing).
[63] *Id.*; Appendix I.
[64] Appendix I.
[65] *Id.*
[66] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1 (prepared testimony and statement of Richard Smith, former Chief Executive Officer, Equifax).
[67] *Mandiant Incident Response*, FIREYE, SERVICES, https://www.fireeye.com/services/mandiant-incident-response.html. Mandiant is an incident response service, dedicated to quick investigations for threat intelligence and network breaches.
[68] *Timeline*, supra note 62, at 3.
[69] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 5; Appendix I.

individual consumers to learn if they were impacted.[70] Finally, on September 7, Equifax notified the general public of the overwhelming scale of the breach and revealed their new consumer support website, a full one hundred and seventeen days after the customer data was first compromised.[71]

To summarize, it took Equifax several months to install a critical software patch after the Department of Homeland Security notified them of the update.[72] It took eleven weeks for Equifax's security team to even notice the suspicious network activity once their system was breached.[73] It took four additional days to contact a law firm and cybersecurity company for the purposes of conducting a comprehensive investigation.[74] After three more weeks, Equifax had the foresight to register a domain name for consumer support, meaning that, at that point, they likely knew the extent of the damage.[75] Despite that knowledge, however, it then took Equifax another two weeks to issue a press release and notify the American public that their most private information had been stolen.[76] In total, twenty-six weeks passed from the date that the Department of Homeland Security issued its warning until Equifax finally announced that its systems had been compromised.[77]

---

[70] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1 (prepared testimony and statement of Richard Smith, former Chief Executive Officer, Equifax); *see also* AnnaMaria Andriotis, Michael Rapaport, & Robert McMillan, *'We've Been Breached': Inside the Equifax Hack,* WALL ST. J. (Sept. 18, 2017), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318?shareToken=st7d9a987129fe43eba2a7852049aab49b&reflink=article_email_share.

[71] *Timeline*, *supra* note 62, at 1-3; Appendix I.

[72] Appendix I.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*; *see also 2017 Internet Security Threat Report*, SYMANTEC (Apr. 2017), https://www.symantec.com/security-center/threat-report. Symantec, a leading cybersecurity and software firm published a 2017 Internet Security Threat Report that compares the time delay of Equifax's actions to other private corporations that suffered breaches. According to this report, the average patch time for organizations is 55 days. It takes an average of six days for exploitable code to become available to the public. Notably, as highlighted in Appendix I, Equifax did not apply the Apache Strut patch for at least 144 days.

[77] *Timeline*, *supra* note 62; Appendix I.

Companies often take liberties when it comes to notifying victims of a breach.[78] They may require additional time to work with law enforcement and attribute the cyber intrusion to a specific threat actor.[79] What is not acceptable, however, is when private corporations prioritize their bottom line over the security and privacy of their customers.[80] In this specific instance, the length of time it took to notify victims, coupled with the intervening sale of $1.8 million in stock, has led some to conclude that corporate executives were attempting to avoid legal consequences while brazenly putting consumers at risk.[81] Thus, in-depth analysis of this data breach requires additional discussion of the duties owed to individual consumers. More importantly, it necessitates a thorough examination of the impact of the Equifax hack on the American collective, specifically the public welfare, economy, and overall national security of the United States.

IV. NATIONAL SECURITY IMPLICATIONS

The national security implications of the Equifax hack are unprecedented. Although this topic has been largely overlooked in the media and in relevant scholarship, such a widespread attack on the American economy could have a profound effect, not just on individual consumers,

[78] 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 ("There are legitimate reasons why a company would choose to wait before going public. Sometimes they are cooperating with law enforcement who don't want to sabotage their investigation into the source of the hack … certain companies can easily prioritize their bottom line over customers' financial security and privacy…. In the case of Equifax, the company's slowness combined with the executives who sold off their stocks prior to the public announcement make the company look like it was minimizing responsibility for a serious consumer problem.").
[79] *Id.*
[80] *Id.*
[81] *Id.*; *see also* Chris Arnold, *Senator to Ex-CEO: Equifax Can't Be Trusted with Americans' Personal Data*, NPR (Oct. 4, 2017), https://www.npr.org/2017/10/04/555651379/senator-to-ex-ceo-equifax-can-t-be-trusted-with-americans-personal-data (highlighting that Equifax has the most consumer bureau complaints in every state but one); Turner, *supra* note 78 ("Companies have often taken liberties with time when notifying customers of a hack. But doing so brazenly puts their customers at risk while these companies avoid consequence.").

but on the general welfare of the nation as a whole.[82] As described above, "Equifax warehouses the most intimate details of Americans' financial lives, from the credit cards in their wallets to the size of their medical bills."[83] Moreover, in recent years, private businesses and corporations have found themselves on the frontline of a new global conflict.[84] The dawn of digital interconnectedness has profoundly benefited our society.[85] Nonetheless, recent technological advances have also emboldened state and non-state actors wishing to do our country harm.[86]

America is on the brink of a crisis. This past August, President Trump's National Infrastructure Advisory Council warned that we have entered a "pre-9/11 cyber moment, with a narrow and fleeting window of opportunity to coordinate our resources effectively."[87] They are not alone in their assessment.[88] The President's recent National Security Strategy also calls for

[82] *See* James G. Hodge, Jr. & Kim Weidenaar, *Public Health Emergencies as Threats to National Security*, 9 J. NAT'L SEC. L. & POL'Y 81, 90 n.60 (2017); *see also* Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International Law,* 40 N.C. J. INT'L L. & COM. REG. 443 (2015). Catherine Lotrionte has written an in-depth review of the impact of economic espionage from foreign states, and the impact on national security. She argues that the United States should not be limited in its countermeasures, yet can seek refuge under the current framework of international law.

[83] Bernard & Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, *supra* note 35; *see also* Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Identity Theft After Clapper v. Amnesty International*, 114 MICH. L. REV. 1471, 1472 (2016) ("We live in a world controlled more than ever by the cybersphere…. As a result the 'intimate details of our lives' – addresses, birth dates, Social Security numbers, and credit card and bank account information – are now stored in online databases.").

[84] Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law*, 8 HARV. NAT'L SEC. J. 239, 242 (2017) (describing cyber operations as a "new domain of conflict"); see also Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DISC. 320, 322 (2016) (discussing the dramatic increase in digital information and proposing a strategic retreat by businesses); Alex Schneider, *How Could They Know That? Behind the Data That Facilitates Scams Against Vulnerable Americans*, 19 VA. J. L. & TECH. 716, 721-22 (2015) (examining the "data broker industry" and debates between privacy advocates and companies).

[85] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422 (2011) (explaining global interconnectedness and the benefits it has brought to our society); James Eastman, *Avoiding Cyber-Pearl Harbor: Evaluating Government Efforts to Encourage Private Sector Critical Infrastructure Cybersecurity Improvements*, 18 COLUM. SCI. & TECH. L. REV. 515, 520 (2017) ("While cyberspace has benefited society tremendously as a source of education and innovation, the private sector's vulnerability to cyberattacks represents one of the most serious national security challenges we must confront.").

[86] Waxman, *supra* note 85 at 422 ("Global interconnectedness brought about through linked digital information networks brings immense benefits, but it also places a new set of offensive weapons in the hands of states and non-state actors…").

[87] THE PRESIDENT'S NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, SECURING CYBER ASSETS: ADDRESSING URGENT CYBER THREATS TO CRITICAL INFRASTRUCTURE 5 (2017) (drft).

[88] See Eastman, *supra* note 85, at 553; Carlin, *supra* note 11, at 393; Reflections on the Tenth Anniversary of the 9/11 Commission Report, BIPARTISAN POLICY CTR. (July 2014), http://bipartisanpolicy.org/wp-

bold, decisive action to protect the "safety, interests, and well-being of our citizens."[89] The administration recognizes that "America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security."[90] Accordingly, we must defend ourselves against state and non-state actors who "use cyberattacks for extortion, information warfare, disinformation, and more."[91] As the strategy notes, these types of attacks "can undermine faith and confidence in democratic institutions and the global economic system."[92]

It is interesting, then, that America's lawmakers chose not to address the regulatory deficiencies that contributed to the Equifax hack.[93] Overall, the law surrounding cyberattacks and data breaches is in its infancy.[94] This situation has also been exacerbated by a lack of clarity in relevant legal definitions.[95] Specifically, the terms "cyberattack" and "data breach" have broad and varying definitions depending on the context, although this article will use an amalgam of definitions for ease of discussion.[96] The phrase "cyberattack" is generally used to describe a hostile activity undertaken by a *state actor*, for a *political or national security purpose*, intended to *alter, disrupt, or destroy* computer systems or networks.[97] "Data breaches," on the other hand,

---

content/uploads/sites/default/files/files/%20BPC%209-11%20Commission.pdf; Leon E. Panetta, U.S. Sec'y of Def., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[89] NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA, *supra* note 17, at 1.

[90] *Id.* at 12.

[91] *Id.* at 31.

[92] *Id.*

[93] Matishak, *supra* note 14.

[94] Waxman, *supra* note 85 at 458 ("Cyber-attacks pose difficult line-drawing problems, but we must avoid missing the strategic forest in thinking about the legal trees."); Schmitt, *supra* note 84 at 242 ("At the heart of this struggle is unfortunate uncertainty as to the applicable law").

[95] *See* Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 826 (2012) (defining the term cyberattack as "any action taken to undermine the functions of a computer network for a political or national security purpose"); Waxman, *supra* note 85, 422 (defining cyberattacks as "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them"); *see also* Stephen Dycus, Congress's Role in Cyber Warfare, 4 J. NAT'L SECURITY L. & POL'Y 155, 162 (2010); CLARKE & KNAKE, *supra* note 11, at 6; COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10–11 (2009).

[96] *See generally* Hathaway & Crootof, *supra* note 95; Waxman, *supra* note 85.

[97] Hathaway & Crootof, *supra* note 95, at 824, 830.

are often relegated to the arena of "cybercrime," or, more precisely, cyber activities conducted by a *non-state actor* in *violation of applicable criminal law*.[98]

Notably, in the context of contemporary data breaches, these definitions can be inaccurate and often result in false distinctions. For example, if a state actor penetrates the defenses of a private corporation like Equifax, they are likely doing so with the intent to harm our national security. The breach and resulting exfiltration of data may also be a crime,[99] but the primary purpose is to exert influence over our government and our citizens at an undetermined time in the future. Moreover, the state actor is not breaching the corporation's network with the intent to alter, disrupt, or destroy those systems.[100] Rather, their goal is to remain undetected for as long as possible, or until such time as they are able to locate unprotected data.[101] This distinction is an important one. In essence, there is no effective term to describe a "data breach" conducted by a state actor for political or national security purposes.[102] Although this activity would be more akin to a traditional "cyberattack," the resulting ambiguity likely contributes to confusion amongst lawmakers, national security practitioners, and members of the general public.

While some contend that "cyberespionage" is the more apt phrase to describe a data breach perpetrated by a traditional nation state, this assertion is also problematic.[103] Attribution for these types of activities has been challenging for investigators, making it difficult to apply a specific label to an activity or forcing some practitioners to use "cybercrime" as a default or

[98] *See* Hathaway & Crootof, *supra* note 95, at 830 (emphasis added).
[99] *Id.* ("Such activities may be criminal—as acts of corporate or political cyber-espionage—but they are not cyber-*attacks*.").
[100] *Id.* at 829-30 ("Neither cyber-espionage nor cyber-exploitation constitutes a cyber-attack because these concepts do not involve altering computer networks in a way that affects their current or future ability to function…. To "undermine the function" of a computer system, an actor must *do more than passively observe a computer network or copy data*, even if that observation is clandestine. The actor must affect the operation of the system either by damaging the operating system or by adding false, misleading, or unwelcome information.").
[101] *Id.*
[102] *See generally id.*; Waxman, *supra* note 85.
[103] Hathaway & Crootof, *supra* note 95, at 829.

interim placeholder.[104] Moreover, it is increasingly difficult to ascertain whether an event was perpetrated by an independent criminal actor or a non-state actor working on behalf of a foreign power, thus making it unclear whether a particular cyber intrusion would ultimately fall under the definition of "cybercrime" or "cyberespionage."[105] Definitions of the term "cyberespionage" vary widely, with some scholars using it as a broad catchall to include the *capture of data or electronic communications* from *corporations* for *national security purposes*.[106] Other definitions, however, stress that the term cyberespionage applies only to the *capture of confidential data* from *government agencies* for *national security purposes*, effectively limiting the definition to classified, public sector information.[107]

Unfortunately, despite this ongoing lack of clarity, the future harm to our national security from these types of activities could be considerable. The 2015 breach of the Office of Personnel Management (OPM), a steward of some of the U.S. government's most sensitive personnel data, demonstrates that "stored information is always at risk and under attack by

[104] *See* Eichensehr, *Giving Up on Cybersecurity*, *supra* note 84, at 371 n.306 (citing Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1573-80 (2010)) ("Without positive attribution, there is no ability to monitor, verify, or signal in the traditional Cold War sense," which "raises the question of whether or not cyber deterrence is even possible at this juncture."); *see also* Taylor Armerding, *Whodunit? In Cybercrime, Attribution Is Not Easy*, CSO ONLINE (Feb. 5, 2015), http://www.csoonline.com/article/2881469/malware-cybercrime/whodunit-in-cybercrime-attribution-is-not-easy.html.

[105] *See* Carlin, *supra* note 11, at 412 ("Computer crimes increasingly resist neat division into criminal and national security categories. Because the identity and goals of the hacker are often unknown at the outset of a cyber intrusion, it is not always possible to segment investigations into clear criminal or national security categories. Many of the same technical, legal, and policy questions arise regardless.").

[106] Hathaway & Crootof, *supra* note 95, at 829 n.48 (citing Seymour M. Hersh, *The Online Threat: Should We Be Worried About a Cyber War*? THE NEW YORKER (Nov. 1, 2010)), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?) ("The science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence.").

[107] *See, e.g.*, Gary Brown, *Spying and Fighting in Cyberspace: What is Which?*, 8 J. NAT'L SEC. L. & POL'Y 621, 622 (asserting that traditional espionage, and by extension cyberespionage encompass "a government's efforts to acquire clandestinely classified or otherwise protected information from a foreign government"); *see also* David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, 17 ASIL INSIGHTS NO. 10 (Mar. 20, 2013) (further explaining that the term "economic espionage" would have no applicability to the Equifax hack, or breaches of consumer PII from credit reporting agencies, because the term applies to a State's attempts to covertly acquire covertly "trade secrets" from private enterprises).

malign actors."[108] While the number of victims in the OPM hack did not surpass that of Equifax, the breach was significant in that it specifically targeted security clearance information for the federal workforce.[109] Thus, the hack itself did not fall under the rubric of a traditional "cyberattack" because threat actors did not directly alter, disrupt, or destroy OPM's computer systems.[110] The catastrophic harm may instead occur at some point in the future, to include "the ability to blackmail, shame, or otherwise coerce public officials."[111]

China ultimately arrested the hackers it claimed were responsible for the OPM hack, although U.S. officials questioned whether the arrests were conducted in an effort to lessen tensions with Washington.[112] The FBI also recently detained a suspect who attempted to enter the United States.[113] Regrettably, what is most troubling about the OPM data breach is that the PII of federal government employees, including sensitive information from background investigations, will never be recovered. This type of harm cannot be undone through subsequent arrest or prosecution. Moreover, some experts contend that the OPM breach was part of a much larger effort on the part of China to assemble a vast database of information for future attacks

[108] Alan Wehbé, *OPM Data Breach Case Study: Mitigating Personnel Cybersecurity Risk*, 26 B.U. PUB. INT. L. J. 75, 93 (2017); *see also* Zachary Figueroa, *Time to Rethink Cybersecurity Reform: The OPM Data Breach and the Case for Centralized Cybersecurity Infrastructure*, 24 CATH. U. J. L. & TECH 433 (2016) ("Politicians continue to decry the OPM Breach as a categorical failure of the Federal Government.").
[109] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ ("Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends.").
[110] Hathaway & Crootof, *supra* note 95 at 829-30.
[111] Wehbé, *supra* note 108, at 86.
[112] Ellen Nakashima, *Chinese Government Has Arrested Hackers it Says Breached OPM Database*, WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.
[113] Evan Perez, *FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach*, CNN (Aug. 24, 2017), https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html.

against the United States, using sensitive information to impersonate or even blackmail federal employees.[114]

As described above, individual consumers can suffer considerable damage if their PII is compromised. When viewed in the collective, however, the 2017 National Security Strategy further acknowledges that cyber events such as the Equifax hack not only impact our security, they also have cascading effects across multiple sectors of the economy.[115] In relevant part, the 2017 National Security Strategy states:

> Over the years, rivals have used sophisticated means to weaken our businesses and our economy as facets of cyber-enabled economic warfare and other malicious activities…. The United States will expand our focus beyond protecting networks to protecting the data on those networks so that it remains secure—both at rest and in transit. To do this, the U.S. Government will encourage practices across companies and universities to defeat espionage and theft.[116]

As President Trump's National Security Strategy stresses, a strong and prosperous economy is essential for the safety and welfare of our citizens.[117] Conversely, a weakened economy can adversely impact our efforts at national defense.[118] Michael Morrell, former Deputy Director of the Central Intelligence Agency, appears to agree with this assessment, noting that "the health of a nation's economy is the single most important determinant in its

[114] Kevin Liptak, Theodore Schleifer, & Jim Sciutto, *China Might Be Building Vast Database of Federal Worker Info, Experts Say*, CNN (June 6, 2015), https://www.cnn.com/2015/06/04/politics/federal-agency-hacked-personnel-management/index.html ("The massive hack that may have stolen the personal information of four million federal employees appears designed to build a vast database in what could be preparation for future attacks by China against the U.S . . . using the stolen personal information to fool and impersonate government workers . . . and blackmail U.S. government officials around the world."); *see also* Nakashima, *supra* note 112 ("U.S. officials have characterized the OPM breaches as traditional espionage — spying to help a foreign government, in this case, build databases on U.S. government employees and officials.").

[115] *See generally* NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA, *supra* note 17.

[116] *Id.* at 21-22.

[117] *Id.*; *see generally* Cameron Ryan Scullen, Note, *Cyberspace: The 21st Century Battlefield*, 6 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 233 (2016) (examining the relationship between the economy and influence across the global sphere).

[118] Ido Kilovaty, *Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the U.N. Charter*, 4 J.L. & CYBER WARFARE 210 (2015) (arguing that the prohibition on the use of force is violated by grave economic cyberattacks, and that economic coercion should be regarded as a national security threat).

ability to protect itself, the single most important determinant in its ability to project power, [and] the single most important determinant in its national security."[119]

Moreover, this fact was not lost on former President Barack Obama when, in the 2015 National Security Strategy, he unequivocally declared:

> America's growing economic strength is the foundation of our national security and a critical source of our influence abroad…. A strong economy, combined with a prominent U.S. presence in the global financial system, creates opportunities to advance our security…. On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government.[120]

This bipartisan emphasis on cybersecurity is revealing. In essence, when a nation introduces austerity measures, or when a country is hindered by economic downturn, that nation has less funding to devote to crucial national security protections.[121] In such a situation, it is imperative to remember that U.S. cyberspace "not only contains our citizens' personal information, but also provides the ability for businesses to maximize their productivity."[122] Thus, private sector prosperity and the personal information of consumers have become inextricably intertwined. When one suffers, it is bound to impact the other as well. PII has therefore proven to be one of the most important pieces of critical infrastructure in our digital age, affecting not only our public welfare, businesses, and economy, but also our overall national security.[123] In the

[119] Michael Morell, *The Link Between Economic and National Security*, THE CIPHER BRIEF (Mar. 13, 2016), https://www.thecipherbrief.com/column_article/the-link-between-economic-and-national-security.
[120] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA (Feb. 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.
[121] *See generally* Gregory Korte, *Trump's 'America First' National Security Strategy Emphasizes Economic Competitiveness*, USA TODAY (Dec. 18, 2017, 5:00 AM), https://www.usatoday.com/story/news/politics/2017/12/18/trumps-national-security-strategy-emphasize-economic-competitiveness/959934001/.
[122] Scullen, *supra* note 117, at 263.
[123] Eastman, *supra* note 85, at 553 ("[T]he government needs to be more assertive in aligning private sector's profit maximization aims with the government's goal of avoiding a 9/11-like cyber event.").

years ahead, this type of data, or the theft and subsequent exploitation thereof, will serve as a crucial determinant of global primacy in modern-day conflicts.

V. OVERVIEW OF THE CURENT LEGAL REGIME

Equifax is currently operating with minimal government oversight,[124] and its corporate executives, responsible for one of the most significant data breaches in U.S. history, are unlikely to face more than a public tongue-lashing by Congress.[125] Credit monitoring agencies occupy what some describe as a "gray area" in government regulation.[126] Many of the data security laws that apply to the banking industry also apply to Equifax.[127] Nonetheless, banks are subject to much stricter oversight, with comprehensive audits and compliance measures administered by a team of outside agencies.[128] Consumer-credit reporting agencies, in comparison, are often subjected to scrutiny only after something has gone terribly wrong.[129]

In the absence of comprehensive federal regulation, enforcement efforts targeting the credit reporting industry are largely left up to individual states.[130] Currently, forty-eight states mandate some sort of consumer disclosure following a data breach, although timing of the notice is only provided for in eight states, and can vary from fifteen to ninety days.[131] The other forty states, including Georgia where Equifax is headquartered, have no timing requirement

[124] Schein & Phillips, *supra* note 19.
[125] Peter J. Henning, *Hack Will Lead to Little, if Any, Punishment for Equifax*, N.Y. TIMES (Sept. 20, 2017), https://www.nytimes.com/2017/09/20/business/equifax-hack-penalties.html ("The worst anyone connected with Equifax may end up facing is a tongue-lashing from Congress.").
[126] Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, *supra* note 46.
[127] *Id.*; Matishak, *supra* note 14.
[128] Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, *supra* note 46 ("[B]anks face much stricter oversight, with a team of agencies working together to audit institutions and monitor their compliance. Non-bank companies, like the credit bureaus, generally are scrutinized only after something has gone wrong.").
[129] *Id.*
[130] Matishak, *supra* note 14.
[131] Turner, *supra* note 78.

whatsoever.[132] Moreover, there is a different disclosure standard in every state, leaving companies and consumers to navigate forty-eight different legal thresholds governing when and how private corporations must inform their customers that their sensitive data has been compromised.[133]

Notably, Equifax was subject to more consumer complaints in 2017 than any other financial services company.[134] Despite this revelation, Congress has done little to unify these various state laws into broad, overarching federal legislation.[135] To be certain, credit reporting agencies are subject to some regulation by the federal government, however, no specific law has been designed to standardize data and information security practices across the entire industry.[136] Consequently, "there are almost no [federal] laws or regulations … that impose stiff penalties for allowing personal data in [the credit reporting agency's] possession to get hacked."[137]

Government oversight efforts within the credit-reporting industry are in substantial need of reform.[138] Additionally, events surrounding the Equifax hack help to further highlight deficiencies within the current legal regime, and in relevant consumer privacy protections.[139] In

[132] *Id.*
[133] Matishak, *supra* note 14.
[134] Sylvan Lane, *Equifax Subject of Most Consumer Bureau Complaints in All but One State: Analysis*, THE HILL (Jan. 11, 2018, 3:47 PM), http://thehill.com/policy/finance/368562-equifax-subject-of-most-consumer-bureau-complaints-in-all-but-one-state.
[135] *See* Matishak, *supra* note 14.
[136] *See* Amy Traub, *The Equifax Hack: We Need to Better Regulate Credit Reporting*, DEMOS (Sept. 11, 2017), http://www.demos.org/blog/9/11/17/equifax-hack-we-need-better-regulate-credit-reporting (describing how some existing regulation may be subsequently rolled back by Congress); *see also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 38 (2018) (defining information security as "a risk management process that security professionals undertake to protect the confidentiality, integrity, and availability of information and information systems.").
[137] Michael Hiltzik, *Before its Massive Data Breach, Equifax Fought to Kill a Rule Allowing Victims to Sue*, L.A. TIMES (Sept. 11, 2017), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-arbitration-20170911-story.html.
[138] Schein & Phillips, *supra* note 19.
[139] *Id.* (describing the different judicial circuit interpretations of the *Fair Credit Reporting Act*, and how this adds to lack of oversight for a changing industry); *see also* Brett V. Newman, Note, *Hacking the Current System: Congress' Attempt to Pass Data Security and Breach Notification Legislation*, U. ILL. J. L. TECH & POL'Y 437, 438 (2015). Newman's article notes at least eight different bills related to cybersecurity, privacy, and information security. In

particular, there are three pieces of legislation relevant to this article's discussion of data breaches.[140] These are the *Financial Services Modernization Act (FSMA),*[141] the *Fair Credit Reporting Act (FCRA),*[142] and the *Federal Trade Commission Act (FTCA).*[143]

A. The Financial Services Modernization Act (FSMA)

The *FSMA* is, ironically, not modern enough to incorporate data security provisions.[144] More commonly known as the *Gramm-Leach-Bliley Act*, the *FSMA* broadly requires financial institutions to insure the security of customer records and information, and to protect this information against anticipated threats and unauthorized disclosures.[145] The Act also allows federal regulators, principally the Federal Trade Commission (FTC),[146] to enforce standards through the "Safeguards Rule," which directs financial institutions to develop written information security plans.[147]

---

nearly all cases, this proposed legislation failed, leaving us with "no comprehensive federal law for data security and breach notification." Newman does not contend that legislation should regulate a company's internal policy. He does, however, call for comprehensive legislation which notifies consumers of breaches, so they can take proactive steps to protect their personal information.

[140] *See generally* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355 (2015) (highlighting consumer privacy protections in the modern era, and how better regulation can increase financial oversight for the benefit of consumers); David C. Vladeck, *Charting the Course: The Federal Trade Commission's Second Hundred Years*, 83 GEO. WASH. L. REV. 2101 (2015) (presenting a brief history of the FTC, and outlining regulatory adjustments that can safeguard a consumer's information privacy as well as combat deceptive advertising); Robert L. Rabin, *Federal Regulation in Historical Perspective,* 38 STAN. L. REV. 1189 (1986) (providing an extensive historical overview of federal financial regulation).

[141] Gramm-Leach-Bliley Act (Financial Services Modernization Act), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in 15 US.C. §§ 6801- 6827 (2006)) [hereinafter FSMA].

[142] Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681(u) (1970) [hereinafter FCRA].

[143] Federal Trade Commission Act, ch. 311, 38 Stat. 717 (1914) (codified at 15 U.S.C. § 41-58 (1964)) [hereinafter FTCA].

[144] *See* FSMA, *supra* note 141.

[145] *Id.*; *see also* Standards for Safeguarding Customer Information, 16 C.F.R. §§ 314.1 –314.4 (2002) [hereinafter Safeguards Rule]; *see also* Scullen, *supra* note 117 at 247 (noting the potential for statutory and civil liability for companies that store data and personal information in cyberspace).

[146] See *About the FTC,* FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (Feb. 3, 2018), https://www.ftc.gov/about-ftc . The Federal Trade Commission works "to protect consumers by preventing anticompetitive, deceptive, and unfair business practices, enhancing informed consumer choice and public understanding of the competitive process, and accomplishing this without burdening legitimate business activity."

[147] 16 C.F.R. § 314.1.

The Safeguards Rule requires that private corporations fulfill five key security requirements to better protect customer information, whereby each company must:

1) Designate an employee or team to coordinate an information security program;
2) Conduct risk assessments of customer information and evaluate the effectiveness of current safeguards for controlling identified risks;
3) Design and implement a safeguards program to address any discovered risks and regularly monitor and test this program's key controls, systems, and procedures;
4) Select and retain service providers that are able to maintain appropriate safeguards of customer information; *and*
5) Evaluate and adjust the safety program as a result of ongoing testing and monitoring.[148]

Although the full scope of liability, if any, for the Equifax breach has yet to be determined, it appears that the company failed to comply with essential elements of the Safeguards Rule.[149] Equifax's designated program manager, who was aware of the software vulnerability, neglected to patch the system for several months, during which time the risk went undiscovered through additional testing and monitoring.[150] As a result, the security regime failed, and malicious actors were able to gain access to sensitive consumer information.[151]

Additionally, there is one added complication related to applying the Safeguards Rule to consumer data held by credit reporting agencies. The *FSMA* is intended to protect "customer information,"[152] however, it is unclear if Equifax even treats its sensitive data as belonging to an actual "customer." When a business or other entity needs to assess the creditworthiness of an individual, they buy this information, and the corresponding credit report, from Equifax.[153] In

[148] 16 C.F.R. § 314.4.
[149] *Id*.
[150] Shepardson, *supra* note 9.
[151] *Id*.
[152] *See generally* FSMA, *supra* note 141.
[153] *See generally* Brooke Niemeyer, *Who Are the Major Credit Reporting Agencies?*, CREDIT.COM (Oct. 26, 2016), https://www.credit.com/credit-reports/credit-reporting-agencies/ (providing a broad overview of credit reporting agencies).

fact, the *FSMA* defines "customer information" as only pertaining to "information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and *is identified with [that] customer*."[154] Here, there is no active relationship between the individual consumer and the company itself.[155] Thus, PII that was compromised as a result of the Equifax hack may not qualify for the *FSMA*'s added protections because the data cannot be considered "customer information" per se.

B. The Fair Credit Reporting Act (FCRA)

The *FCRA* is designed to apply directly to credit reporting agencies.[156] Nonetheless, it falls far short of implementing comprehensive data security measures, requiring only that credit reporting agencies "make reasonable efforts to verify" the identity of those requesting consumer credit reports.[157] While the *FCRA* does mandate some minor "diligence requirements," it contains no discernable provisions specifically intended to apply to data and information security.[158] Furthermore, although the FTC retains enforcement authority under the *FCRA*,[159] the Consumer Financial Protection Bureau (CFPB) has subsumed a large portion of its rulemaking

[154] 15 U.S.C. § 6827 (emphasis added).
[155] CONSUMER FINANCIAL PROTECTION BUREAU, *supra* note 30.
[156] *See generally* FCRA, *supra* note 142; *see also* Schneider, *supra* note 84, at 743-45. Schneider proposes that the credit reporting industry needs to be reformed, not just in cybersecurity practices, but in the credit industry's sale of personal data to brokers, which remains a largely unregulated practice. Schneider's prime criticism is that consumer reporting requirements in the FCRA only apply to those reports issued to consumers, not "other reports, such as a data broker reports used for marketing purposes."
[157] 15 U.S.C. § 1681(e); *see generally* Edward Thrasher, *The Fair Credit Reporting Act: Deficiencies and Solutions*, 21 TEMP. POL. & CIV. RTS. L. REV. 599 (2012) (outlining a number of legal issues in the credit reporting process, including how some innocent citizens are falsely labeled as a threat to national security and then must work to clear their name).
[158] *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, 176 (2008). Scott highlights some of the more recent FTC investigations directed against companies for security breaches under its unfairness doctrine. Yet, he also suggests that the enforcement regime is applied at random. Scott also proposes that new legislation should expand the FTC's authority, however only under strict regulations and guidelines, so as to clarify the role the FTC should play in countering cybersecurity threats.
[159] *Fair Credit Reporting Act*, FED. TRADE COMMISSION, https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act.

authority in recent years, creating additional operational ambiguities when it comes to federal enforcement efforts.[160]

Particular shortcomings in this legislation, and in its applicability to large-scale data breaches, should be evident from circumstances surrounding the Equifax hack. Companies required to employ "reasonable efforts" at data and information security are given substantial discretion to decide what is reasonable under the circumstances. The law "provides little or no guidance on what specific security measures are required or on how much security a business should implement to satisfy [these] legal obligations."[161] The resulting information security program may therefore be deficient when contrasted against current data security norms or best practices. Furthermore, the FTC's investigative purview does not extend to proactively inspecting credit reporting agencies for lax cyber defenses or adherence to the Safeguards Rule.[162] Rather, it is a reactionary agency, charged with investigating data breaches only after they occur.[163]

To further complicate matters, federal courts have offered limited guidance on the *FCRA* as it relates to data breaches within the credit reporting industry. In interpreting the language of the *FCRA*, the U.S. District Court for the Northern District of Georgia held in *Willingham v. Global Payments, Inc.* that if a credit reporting agency does not "furnish" or "transmit" consumer

[160] *See* Virginia G. Maurer & Robert E. Thomas, *Getting Credit Where Credit is Due: Proposed Changes in the Fair Credit Reporting Act*, 34 AM. BUS. L. J. 607 (1997) (giving a brief history of rulemaking versus enforcement authority of the FTC and CFPB, and explaining how responsibilities of the FRCA should not fall solely on credit reporting agencies, but also on information purchasers); *see also* Appendix II – *Comparison Chart of Relevant Investigative Authorities* (providing a detailed breakdown of FTC and CFPB authorities versus the new agency proposed in this article).
[161] Thomas J. Smedinghoff & Ruth Hill Bro, *Lawyers' Legal Obligations to Provide Data Security*, *in* RHODES & LITT, *supra* note 136, at 65.
[162] Evan Weinberger, *Senators Back More Oversight of Credit Bureau Cybersecurity*, LAW360 (Oct. 17, 2017), https://www.law360.com/articles/974981/senators-back-more-oversight-of-credit-bureau-cybersecurity *citing to Oversight of the Equifax Data Breach: Answers for Consumers*, *supra* note 1.
[163] *Id.*

data directly to hackers, then liability does not attach.[164] Thus, Equifax may also have the ability to claim that PII from the hack was simply "stolen, not furnished," subsequently avoiding any responsibility for the breach.[165] When you consider the lack of specificity in the *FCRA*, as well as relevant legal precedent in *Willingham*, you are left with a legislative framework that fails to properly protect consumers against ongoing cyber risk.

C. The Federal Trade Commission Act (*FTCA*)

The *FTCA* serves as the authorizing statute for the Federal Trade Commission (FTC) and prohibits "unfair or deceptive acts or practices in or affecting commerce."[166] This effectively bars companies from making false or misleading claims regarding data protections they provide to their customers.[167] Moreover, this section of the *FTCA* authorizes the FTC to target companies that utilize unfair practices likely to cause consumers substantial injury.[168] Nonetheless, as it relates to victims of the Equifax data breach, it is unclear if this section of the *FTCA* extends to implementation and maintenance of information security programs.[169] In this particular instance, it also does not appear that Equifax made any deceptive claims or representations to customers regarding their data security practices.[170]

---

[164] *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013).
[165] *Id*. at *46. District Judge King seized on the language of the *FCRA*, noting that "furnishing" data involves a willing transmission of that data to a third party.
[166] 15 U.S.C. § 45.
[167] *Id.*; *see also* Merritt Baer & Chinmayi Sharma, *What Cybersecurity Standard Will a Judge Use in Equifax Breach Suits?* LAWFARE BLOG (Oct. 20, 2017, 7:30AM), https://www.lawfareblog.com/what-cybersecurity-standard-will-judge-use-equifax-breach-suits.
[168] Baer & Sharma, *supra* note 167.
[169] *Id.*; *see* also Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2289–99 (2015) (providing a comprehensive outline of the FTC's regulatory enforcement authority and postulating that the FTC should have more discretion to push the boundaries of their current enforcement authorities, thus helping to create essential cybersecurity norms across more industries).
[170] FEDERAL RESERVE, FEDERAL TRADE COMMISSION ACT SECTION 5: UNFAIR OR DECEPTIVE ACTS OR PRACTICES, CONSUMER COMPLIANCE HANDBOOK (Dec. 2016), https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

Equifax is currently subject to an FTC investigation regarding their handling of the data breach.[171] The Securities and Exchange Commission is also conducting an insider trading inquiry of top officials at the company.[172] Moreover, the CFPB launched a probe into the efficacy of Equifax's data security program.[173] At present, more than 350 class action lawsuits have been filed by consumers, with six teams of attorneys vying for top billing amongst the various plaintiffs.[174] Although such lawsuits may ultimately succeed in achieving increased consumer protections, these myriad investigations are contributing to an environment in which agency jurisdiction and investigative authority are uncertain.[175] In February 2018, concerned lawmakers openly voiced their frustrations, questioning investigators at length on why they had not "ordered subpoenas against Equifax or sought sworn testimony from executives, routine steps when launching a full-scale probe."[176]

The FTC does not proactively require that data security measures be up-to-date, and it acknowledges "that reasonable security is a continuous process of assessing and addressing

[171] *FTC Opens Probe Into Massive Equifax Hack*, REUTERS (Sept. 14, 2017, 9:28 AM), https://www.reuters.com/article/equifax-cyber-ftc/u-s-ftc-opens-probe-into-massive-equifax-hack-idUSFWN1LV0KN.
[172] Hayley Tsukayama, *Equifax Faces Hundreds of Class-Action Lawsuits and an SEC Subpoena Over the Way it Handled its Data Breach*, WASH. POST (Nov. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/?utm_term=.63ebac186ff5.
[173] Yuka Hayashi, *CFPB Chief Says Equifax Probe Continues*, WALL ST. J. (Feb. 13, 2018), https://www.wsj.com/articles/cfpb-chief-says-equifax-probe-continues-1518556186.
[174] Amanda Bronstad, *6 Lawyer Teams Vie for Leadership Posts in Equifax Data Breach*, DAILY REPORT (Feb. 5, 2018 7:32PM), https://www.law.com/dailyreportonline/sites/dailyreportonline/2018/02/05/6-lawyer-teams-vie-for-leadership-posts-in-equifax-data-breach/.
[175] *See* Peter S. Frechette, *FTC v. Labmd: FTC Jurisdiction Over Information Privacy is "Plausible," But How Far Can It Go?* 62 AM. U. L. REV. 1401, 1413-15 (2013) (noting that Section 5 of the FTCA gives "fluid jurisdiction" to the FTC but concluding that such authority may open it up to criticism and legal challenges that it is exceeding its jurisdiction); Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207 (2016) (offering a critique of recent FTC legislative recommendations and the plausibility of regulating the entirety of the 'big-data' industry).
[176] Patrick Rucker, *Exclusive: U.S. Consumer Protection Official Puts Equifax Probe on Ice – Sources*, REUTERS (Sept. 8, 2017, 1:14 AM), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.

risks."[177] Moreover, the FTC recognizes that "the mere fact that a breach occurred does not mean that a company has violated the law."[178] When a small or medium-sized company suffers a breach, it may be able to compartmentalize the damage.[179] When one of the largest consumer reporting agencies in the world suffers a breach, the lasting national security implications are likely irreparable.[180] Thus, it is imperative that lawmakers and U.S government officials take a comprehensive approach to government reform in the wake of the Equifax breach. What is needed most is a novel and creative proposal that turns our current reactive stance on corporate security into an active model of cyber defense.

VI. **RECOMMENDATIONS FOR REFORM**

Detractors of the federal government and its dedicated career workforce typically have great success pointing out the inherent shortcomings of a particular government program or process. This is due in part to the public nature of modern allegations of wrongdoing. Accusations often play out explosively in the media, leaving little opportunity for program officials to offer a well-reasoned and accurate defense. Scholars are not immune to this phenomenon, with prominent academics racing to publish on the most controversial topics, or to establish their supremacy on the evening news, acting as talking heads for major cable news networks. Unfortunately, few critics have the ability to offer achievable and creative strategies for improving overall government operations.

---

[177] *Protecting Consumer Information: Can Data Breaches Be Prevented?, Hearing Before the Comm. on Energy and Commerce*, 113th Cong., 2nd Sess. (2014) (prepared statement of Hon. Edith Ramirez, the Chairwoman of the Federal Trade Commission).
[178] *Id*.
[179] *How Middle Market Firms Can Deal with Data Security Breach Threats*, WASH. POST (Dec. 5, 2016), http://www.washingtonpost.com/sf/brand-connect/wp/2016/12/05/cit/how-middle-market-firms-can-deal-with-data-security-breach-threats/?utm_term=.c3eddf97b7ac.
[180] Hautala, *supra* note 47.

We are on the verge of a national security crisis of September 11th proportions.[181] The list of victims from cyber incidents is staggering and includes private corporations, federal and state governments, and individual American citizens.[182] Moreover, the threat has evolved into an existential one, affecting the very fabric of our economy and the well-being of our general populace.[183] The private sector currently owns or operates 85 percent of America's critical infrastructure.[184] Without additional regulation, this places it "outside of the government's direct control and protection, thereby creating a substantial national security conundrum for the entire federal government."[185] This article asserts, however, that until private corporations take independent initiative to improve their data security practices, the federal government has an inherent duty to protect its citizens.[186]

The following recommendations offer a workable blueprint for worthwhile government reform. They are not intended to be inclusive of all possible contingencies, but instead represent a model that is adaptable to multiple industries. The Equifax hack and other recent events should serve as a warning to the American public. Deficiencies in our existing cybersecurity approach simply necessitate a change, not just in applicable law, but also to the underlying structure and function of our government as a whole. These essential reforms will result in an America that is better equipped, and more agile, for the imminent national security challenges to come.

A. Recommendation #1 - Establish a New Bipartisan Commission

[181] *See* THE PRESIDENT'S NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, *supra* note 87, at 5; Eastman, *supra* note 85, at 553; Carlin, *supra* note 11, at 393; *see generally* BIPARTISAN POLICY CTR., *supra* note 88; Panetta, *supra* note 88.
[182] *See generally* NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA, *supra* note 17.
[183] Eastman, *supra* note 85, at 520.
[184] *Id.* at 516.
[185] *Id.* at 520.
[186] *See also id.* at 553.

> *Congress should enact comprehensive legislation that establishes a new bipartisan commission charged with examining cyber incidents and cyber threats across America's public and private sectors. This commission should be given a broad legislative mandate to research and examine information security practices within government agencies and private sector corporations. It should also have the authority to proactively issue recommendations targeting perceived vulnerabilities in existing cyber defenses.*

Congress created the National Commission on Terrorist Attacks upon the United States (the 9/11 Commission) to conduct the herculean task of investigating the facts and causes relating to the terrorist attacks of September 11, 2001.[187] Commission members were required to "ascertain, evaluate, and report on the evidence developed by all relevant governmental agencies."[188] Furthermore, they were directed to "make a full and complete accounting of the circumstances surrounding the attacks, and the extent of the United States' preparedness for, and immediate response to, the attacks."[189] The resulting report contained a damning assessment of U.S. intelligence failures and also called upon American lawmakers and citizens alike to embrace a new system of government, one that valued unity of effort and the security of our nation above petty partisan disagreements.[190]

The 9/11 Commission cautioned that America can never again become complacent or overlook telltale warning signs alerting us to an imminent and devastating national security event.[191] Commission members advised Americans "to remember how we all felt on 9/11, to remember not only the unspeakable horror but how we came together as a nation – one nation."[192] Additionally, they solemnly requested that we never forget the more than 2600

[187] Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, 116 STAT. 2383, § 602 (2002).
[188] *Id.*
[189] *Id.*
[190] *See* STAFF OF NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 108TH CONG., THE 9/11 COMM'N REP. (2004) [hereinafter 9/11 COMM'N REP.].
[191] *Id.* at 26.
[192] *Id.*

innocent people murdered at the World Trade Center, the 125 people who perished at the Pentagon, and the 256 passengers who died on the four hijacked aircraft.[193] Despite this powerful admonishment, we are dangerously close to repeating the past.

America's lawmakers should enact comprehensive legislation to establish a new bipartisan commission in advance of the next catastrophic attack. This commission should be charged with examining the current state of cybersecurity in both the public and private sectors. While it will investigate the Equifax data breach as part of a broader study, commission members should remain forward-looking and proactive. They should examine the root causes and vulnerabilities that contributed to several of the most damaging cyberattacks and data breaches in recent history. More importantly, they should instill lessons learned and relevant countermeasures into future cyber defenses in an attempt to ward off a largescale cyber event. Accordingly, the commission's mandate should not be limited to cyberattacks and cyberespionage perpetrated by traditional nation states, or data breaches caused by individual criminal actors. Rather, these types of incidents should be given equal scrutiny, accounting for the growing ambiguities between conventional state actors and cybercriminals acting as proxies for foreign powers.[194]

Similarly, the commission should examine threats to both government systems and those of private corporations. The nature of the global threat landscape necessitates that America's

[193] *Id*. at 1-2.

[194] *Cyber Security: Responding to the Threat of Cyber Crime and Terrorism*: *Hearing Before the S. Subcomm. on Crime and Terrorism, Comm. on the Judiciary*, 111th Cong., 1st Sess. (2011) (statement of Gordon Snow, Assistant Director of the Federal Bureau of Investigations Cyber Division) (addressing the interrelationship between cybercriminals and state actors and explaining that "[t]he botnets run by criminals could be used by cyber terrorists or nation states to steal sensitive data, raise funds, limit attribution of cyber attacks, or disrupt access to critical national infrastructure."); *see also* Carlin, *supra* note 11, at 412 ("We continue to see the threats and motivations blending. We see individual hackers supporting terrorist aims, groups defacing websites and simultaneously profiting from their criminal activities, and increasingly the lines between state actor, criminal group, and terrorist are blurring.").

public and private sectors be examined in tandem.[195] Whether they are targeting a system used by a government agency or a private corporation like Equifax, malicious actors often use the same tools and techniques to gain unauthorized access.[196] Subsequently, legislators should not diminish the impact of this new commission by imposing strict limitations related to the origin or source of a cyber intrusion. They should instead allow the commission adequate independence and flexibility to adapt its investigation and subsequent recommendations to the ever-changing spectrum of emerging threats.

Given the current political climate, lawmakers will be reluctant to grant a commission such wide-ranging and expansive authority. They will also contend that such legislation is unworkable or that the commission's mandate is overbroad. When faced with the prospects of an attack as devastating as that of September 11, 2001, however, this article respectfully requests that they reconsider. Each Member of Congress has had constituents victimized by the Equifax hack and other major data breaches.[197] This issue also touches upon the jurisdiction of several different congressional committees.[198] In this instance, a bipartisan commission allows neutral factfinders to remain immune from special interests and to proactively determine the correct path forward, absent the continued distraction of partisan political disputes.[199] Furthermore, it embodies the current administration's stated objective of protecting "the American people, the American way of life, and American interests."[200]

---

[195] *Id.*
[196] *Id.*; s*ee also* Riley Walters & Mike Muller, *State Actors Are Likely Behind Recent Ransomware Attacks*, HERITAGE (July 26, 2017), https://www.heritage.org/cybersecurity/commentary/state-actors-are-likely-behind-recent-ransomware-attacks (clarifying that both state actors and cybercriminals use Ransomware, a type on malware that locks computers until ransoms are paid, although the underlying motivation for these two actors often differs).
[197] Matishak, *supra* note 14 ("Certainly, every member here has had constituents that have been victims of these breaches…").
[198] *Id.*
[199] *See generally* 9/11 COMM'N REP., *supra* note 190.
[200] NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA, *supra* note 17, at 7.

B. Recommendation #2 - Create a New Information Security Agency

As part of its comprehensive legislation, Congress should create a new Information Security Agency tasked with overseeing the implementation of the commission's recommendations. This agency should be given the statutory authority necessary to effectively oversee information security practices within both government agencies and private corporations. Within the Information Security Agency, Congress should also establish a Financial Security Section that focuses exclusively on improving data security practices within the financial services industry.

As part of the comprehensive legislation described above, Congress should create a stand-alone executive branch agency authorized to oversee and enforce compliance with the commission's recommendations. This new Information Security Agency should focus exclusively on improving information security practices within the public and private sectors. Consequently, it will be comprised of three principal divisions – the Public Sector Data Security Division, the Private Sector Data Security Division, and the Policy and Planning Division.[201] While the first two divisions will focus on implementing recommendations directed to the public and private sectors, respectively, the Policy and Planning Division will have cross-cutting responsibilities, conducting research and planning for emerging threats in both sectors. This will enable agency personnel to identify patterns amongst various threat actors, contributing to overall cyber attribution efforts. It will also facilitate effective information sharing by ensuring that private corporations are not vulnerable to malicious actors already known to the government, and vice versa.

This new agency should remain fully transparent to consumers, have regular congressional reporting requirements, and be built upon specific statutory safeguards to prevent lobbying influence and corruption. Within the Private Sector Data Security Division, Congress

[201] *See* Appendix III - *Proposed Organizational Chart for the Information Security Agency* (describing the organizational chart for the proposed Information Security Agency).

should establish a Financial Services Section to oversee compliance measures within the financial services industry. While the commission retains the right to recommend additional modifications to this section's organizational structure, it should, at a minimum, be given legislative authority to enforce penalties against companies that disregard applicable security regulations or fail to report major data breaches to government agencies within a 7-day period.[202] The section should also implement incentives for compliance with existing regulations and the effective disclosure of breaches. Moreover, section personnel can help to educate the general public by producing publicly available reports that identify simple methods for consumers to protect their identity, credit information, and overall internet presence. Ideally, the Information Security Agency should strive to create a minimum standard of cyber care across various industries which can be immortalized in future legislation.

Congress should also ensure a robust funding mechanism for the newly-established Information Security Agency. This agency should have adequate resources and staffing, combining collocated personnel from all major government entities tasked with safeguarding the United States' information security systems. Individual detailees[203] with subject matter expertise would therefore serve in rotational billets at the agency and act as liaisons to their parent organizations to facilitate effective information sharing. This would allow its Financial Security

[202] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (Mar. 2007); Natasha Lomas, *Equifax Breach Disclosure Would Have Failed Europe's Tough New Rules*, TECH CRUNCH (Sept. 8, 2017), https://techcrunch.com/2017/09/08/equifax-breach-disclosure-would-have-failed-europes-tough-new-rules/. Although several penalty provisions already exist in the United States at the state level, this article is proposing a 7-day statutory requirement to report suspected data breaches to a government institution overseeing such conduct. This requirement is considerably more lenient than the European Union requirement that companies notify customers within 72 hours after a data controller becomes aware of an intrusion.

[203] U.S. OFF. OF PERSONNEL MGMT., THE GUIDE TO PROCESSING PERSONNEL ACTIONS 46 (Mar. 2017), https://www.opm.gov/policy-data-oversight/data-analysis-documentation/personnel-documentation/processing-personnel-actions/gppa14.pdf (explaining that a "detail" is a temporary assignment to a different position for a specified period when the employee is expected to return to his or her regular duties at the end of the assignment … an employee who is on detail is considered for pay and strength count purposes to be permanently occupying his or her regular position).

Section to function as a focal point for all information related to ongoing cybersecurity efforts within the financial services industry. Moreover, participation in the section should not be limited to traditional stakeholders such as the FTC and CFPB. Rather, it should effectively incorporate employees from several intelligence community elements including the Federal Bureau of Investigation.[204] This will help to infuse compliance efforts with timely and accurate intelligence regarding emerging cyber threats.[205]

In terms of the overall chain of command, the President of the United States should also have the unique ability to temporarily elevate the Director of the Information Security Agency to cabinet-level status when required.[206] Such an arrangement is not without precedent and will enable a more effective response to large-scale cyber events by granting the Director a clear line of communication with the President during times of crisis. Furthermore, it will serve as a symbol of the President's confidence in this new government institution, providing the Director with augmented political capital when negotiating with other agency principals. Thus, the Director of the Information Security Agency will be empowered, not only to enact a proactive compliance regime upon government agencies and private corporations, but also to execute an effective all-hazards response to a national security event of September 11th proportions.

---

[204] *See generally* Exec. Order No. 12,333, 3 C.F.R. § 200 (1982), *reprinted in* 50 U.S.C. § 401 note (Supp. V 1981), *amended by* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008) (listing the Federal Bureau of Investigation amongst various intelligence community elements).

[205] *Id.* (describing the value of collecting timely and accurate intelligence and incorporating this information into valuable intelligence products).

[206] *See, e.g.*, Gary Borg, *Fema Director Elevated To Cabinet*, CHICAGO TRUBUNE (Feb. 27, 1996), http://articles.chicagotribune.com/1996-02-27/news/9602270243_1_cabinet-james-lee-witt-white-house-official (describing the President's authority to elevate the Administrator of the Federal Emergency Management Agency to cabinet level status); Bill McAllister, *FEMA Chief Given Cabinet Status*, WASH. POST (Feb. 27, 1996), https://www.washingtonpost.com/archive/politics/1996/02/27/fema-chief-given-cabinet-status/04de4b97-6a71-4ab1-8931-6185559882db/?utm_term=.bc604d292c5f ("Barely two weeks after he heard officials in flood-ravaged states lavish praise on the federal government's disaster coordinator, President Clinton elevated him to be a member of his Cabinet"); DEP'T OF HOMELAND SEC. OFF. OF INSPECTOR GEN., OIG-09-25, FEMA IN OR OUT? 1, 14-16 (2009) ("In 1996, 3 years into Witt's tenure, President Clinton elevated FEMA's status to a Cabinet-level agency. FEMA was then what some are calling for now–an independent, Cabinet-level agency, with a director who had a direct line to the President.").

C. Recommendation #3 – Enhance Current Information Security Oversight

Congress should enhance the statutory authority of both the Federal Trade Commission and the Consumer Financial Protection Bureau as it relates to information security oversight. This legislation should allow both agencies to be more proactive and preventative in their investigative efforts and also provide the FTC increased authority to inspect and audit financial services companies for noncompliance with the Safeguards Rule.

Thus, while the preceding recommendations represent broad-based strategic solutions to national security vulnerabilities, the following suggestion is designed as a short-term remedy for current investigative efforts conducted by the FTC and CFPB. Specifically, Congress should authorize both agencies to take a more rigorous approach to information security oversight of the credit reporting industry. These private companies handle an extraordinary amount of sensitive data on consumers.[207] They also store and manage a vast amount of PII to include consumers' names, Social Security numbers, birth dates, addresses, and driver's license numbers, or to be more precise, the exact type of information compromised in the Equifax hack.[208] The FTC and CFPB need the authority to proactively monitor the private sector's care and maintenance of this data. More specifically, the FTC should have statutory authority to inspect and audit credit reporting companies like Equifax for noncompliance with the Safeguards Rule.

While the FTC and CFPB have concurrent investigative jurisdiction over events such as the Equifax hack, rulemaking authority for credit reporting agencies rests with the CFPB.[209] Congressman Jerry McNerney stressed this point when asking former Equifax CEO Richard

[207] *See generally* Bils, *supra* note 6; *see also* Newcomb, *supra* note 8.
[208] *See* Newcomb, *supra* note 8.
[209] *See* Maurer & Thomas, *supra* note 160; *Oversight of the Equifax Data Breach Hearing*, *supra* note 1 (statement of Rep. Greg Walden, Chairman, Comm. on Energy and Commerce); see also Appendix II – Comparison Chart of Relevant Investigative Authorities [hereinafter Appendix II].

Smith, "should [the FTC] have rulemaking authority … [W]ould [it] have made a difference?"[210] This article posits that it would have made a substantial difference when it comes to oversight of private sector information security programs. Division of labor between the FTC and CFPB is problematic when it comes to data breaches. Once a company is exposed to a breach, they can be held liable by FTC enforcement actions.[211] The CFPB, however, possesses the relevant rulemaking authority.[212] In practice, this means that a breakdown in communication can result in rules that cannot be effectively enforced and enforcement activities that stray from the rule's original intent.[213]

While comprehensive legislation is required to protect against these known vulnerabilities, this article recognizes that, given the current political climate, America's lawmakers will be hesitant to take such bold action.[214] The FTC and CFPB are currently charged with protecting American consumers. Their respective investigative activities, however, tend to overlook the national security significance of widespread and pervasive cyber intrusions. As described above, national security and the consumer economy are inextricably intertwined.[215] A nation that is crippled by the constant risk of data loss, identity theft, and economic uncertainty will not be able to adequately protect itself from national security threats.[216] Thus, although strengthening the statutory authorities of the FTC and CFPB is an important short-term measure,

[210] *Oversight of the Equifax Data Breach Hearing*, *supra* note 1, at 85.
[211] *See* FED. TRADE COMM'N, *supra* note 146.
[212] *See* CONSUMER FINANCIAL PROTECTION BUREAU, RULEMAKING, https://www.consumerfinance.gov/policy-compliance/rulemaking/.
[213] *See* Appendix II (contrasting authorities of the FTC and CFPB against the proposed Information Security Agency).
[214] Rucker, *supra* note 176 (revealing that congressional inaction on the Equifax breach is still occurring, even with the prospect of a foundering CFPB investigation into the company).
[215] *See* NATIONAL SECURITY STRATEGY FOR THE UNITED STATES OF AMERICA, *supra* note 17 at 17-23.
[216] *Id.*

it is imperative that such reforms only be implemented within the whole-of-government approach outlined in this article.

D. Recommendation #4 – Implement a Minimum Standard of Cyber Care

The newly-created Information Security Agency should strive to establish a minimum standard of care for cyber and data security within the credit reporting industry and should incorporate the common cyber language developed in the Cybersecurity Framework. Congress should then immortalize this standard of care in subsequent legislation.

Senator Mark Warner is one of the few lawmakers calling for Congress to rethink its data protection policies for credit reporting companies.[217] He recommends that Congress establish an industrywide standard of cyber care instead of relying on the judicial branch of government to provide piecemeal court determinations.[218] Overall, judicial precedent has offered mixed results when it comes to data security. Some courts have held that a minimum standard of cyber care exists based in part on the application of a contract law theory of negligence.[219]

In *In re Hannaford*, data thieves stole "4.2 million debit and credit card numbers, expiration dates, security codes, [and] PINs" from a grocery store's electronic payment processing service.[220] The U.S. District Court for the District of Maine subsequently used a

[217] *See, e.g.*, Allison Grande, *Senate Bill Would Up Internet Of Things Device Security*, LAW360 (Aug. 2, 2017, 8:57 PM), https://www.law360.com/articles/950047/senate-bill-would-up-internet-of-things-device-security (outlining Warner's work on a standard of care for the "Internet of Things," or the interconnection via the Internet of computing devices embedded in everyday objects).

[218] *Id.*; *see also* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553 (2005). Rustad and Koenig offer an extensive overview of a new tort in cybercrime, which they call "negligent enablement of cybercrime." The article stems from the increasingly common *and*sophisticated nature of cyberattacks, and the article proposes passing off secondary liability to software companies who "aid and abet cyber criminals." While this proposal is ambitious, there is also merit in the idea of sharing the blame "between the software industry and the user community" when it comes to inadequate computer security.

[219] Merritt Baer & Chinmayi Sharma, *Does Equifax Owe Victims a Duty of Care?*, LAWFARE BLOG (Sept. 12, 2017), https://www.lawfareblog.com/does-equifax-owe-victims-duty-care (outlining verious causes of action in the Equifax breach).

[220] *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 116 (D. Me. 2009).).

negligence theory to uphold a standard of care based on breach of an implied contract.[221] This is a positive development for consumers, as an implied contract may be needed to establish a link between a business used by a consumer, and a credit reporting agency that in turn uses that consumer's data for credit checks and other services. The courts have also applied a failure to act theory in relevant precedent. Specifically, in *Bell v. Blizzard Entertainment Inc.*, the U.S. District Court for the Central District of California upheld a claim of unjust enrichment when a video game company knowingly sold a flawed game to consumers, allowing hackers to obtain customers' email addresses and answers to personal security questions.[222] In that instance, the court found liability because Blizzard took no proactive steps to improve the security flaw once they had knowledge of its existence.[223]

As noted, however, leaving the standard of cyber care solely to judicial interpretation has also resulted in unpredictable outcomes. In *Willingham v. Global Payments, Inc.*, for example, the U.S. District Court for the Northern District of Georgia held that a payment processor owed no duty to consumers who used the company's services to send funds to merchants.[224] In *In re Zappos*, the U.S. District Court for the District of Nevada declined to treat a company's own terms of service as binding, and subsequently denied the existence of an implied contract that safeguarded consumer data.[225] Even more troubling, in *Dittman v. University of Pittsburgh Medical Center*, a Pennsylvania Superior Court held that a medical center did not owe a duty of care to protect the PII of 64,000 employees.[226] Without the benefit of relevant federal precedent, the judge expressly found that it was "unnecessary to require employers to incur potentially

[221] *Id.*
[222] *Benjamin Bell v. Blizzard Entertainment, Inc.*, Case No. 12-CV-09475 BRO (PJWx) (C.D. Ca, 2013).
[223] *Id*.
[224] *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *61 (N.D. Ga. Feb. 5, 2013).
[225] *In re Zappos.com, Inc.* 893 F. Supp. 2d 1058, 1066 (D. Nev., 2012).
[226] Dittman v. UPMC, Civil Division at No. GD-14-003285, 154 A.3d 318, 323 (Super. Ct. of Pa. 2016).

significant costs to increase security measures when there is no true way to prevent [data] breaches altogether."[227]

Congress should authorize the newly-created Information Security Agency to develop a minimum standard of cyber care for the credit reporting industry. It can then be immortalized in future legislation. The resulting standard should govern not only relationships between consumers who have direct interactions with a business, but also business models similar to that of Equifax, in which consumers often have no relationship with a particular company.[228] In establishing this minimum standard of care, the Information Security Agency should consider a variety of factors, including the sensitivity and volume of the data at risk, as well as future harm to consumers.[229] Congress should also grant the Information Security Agency enforcement authority over this standard to ensure the overall compliance of credit reporting agencies.

Moreover, Congress should utilize the "common language" of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to inform subsequent legislation.[230] The Cybersecurity Framework serves as "a set of industry standards and best practices to help organizations manage cybersecurity risks [and] … enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management."[231] More importantly, the Framework applies a "common language for understanding, managing, and expressing

[227] *Id.* at 324.
[228] Bernard & Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, *supra* note 35.
[229] *See* Sean L. Harrington, *Why the Equifax Breach Could Be the Tipping point*, 32 No. 3 WESTLAW J. WHITE-COLLAR CRIME 3, 3 (2017) (noting that such factors "include the sensitivity and volume of the data at risk, the potential for future harm, the status [of the company in question], the monetary resources … available", and related facts available).
[230] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. While this article utilizes the 2014 version of the framework, an updated draft version of the Cybersecurity Framework was circulated for comment in December 2017.
[231] *Id.* at 1.

cybersecurity risk."[232] In May 2017, President Trump issued an executive order requiring the adoption of the Cybersecurity Framework in all executive branch agencies.[233] Private sector corporations, however, have been slow to embrace these standards.[234]

While the common language of the Cybersecurity Framework is admittedly an incomplete solution, commentators note that it "is a step that can be taken collectively, right now, to leverage the collaborative work that has been done and focus attention on specific issues in a more coherent way."[235] Moreover, as the Equifax breach demonstrates, an organized response or common plan for cyber defense is clearly preferable to complete inaction.[236]

E. Recommendation #5 – Design a Cyber Hygiene Public Awareness Campaign

> *The FTC, the CFPB, and the newly-created Information Security Agency should begin a concerted public awareness campaign within the credit reporting industry, marketed to both companies and consumers, educating them on simple cyber hygiene and information security practices. These agencies should update the campaign whenever necessary to account for relevant current events or the evolving spectrum of cyber threats, so as to mitigate the risk of future data breaches.*

The common lesson from every major data breach, including the Equifax breach, is that mere awareness of cyber hygiene and information security practices is not enough to protect a

---

[232] *Id.* at 7.
[233] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (2017).
[234] *The Partnership Between NIST and the Private Sector: Improving Cybersecurity*: *Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong., 2nd Sess. (2013) (statement of Dr. Patrick Gallagher, former Director of NIST) (acknowledging NIST's awareness that the bulk of critical and cyber infrastructure in the United States is owned and operated by private organizations and appealing to companies of all sizes to adopt the common language of the Framework).
[235] Rebekah Lewis, *The Equifax Breach: Getting From Talk to Organized Response*, LAWFARE BLOG (Sept. 29, 2017), https://www.lawfareblog.com/equifax-breach-getting-talk-organized-response. Lewis has argued that the language of the debate over the Cyber Framework is the problem itself. When Congress tries to investigate a matter, they use different language than cybersecurity professionals (for example, "breach" vs."hack"; "compromise" vs. "loss", etc.). Lewis argues that this makes the problem needlessly complex, and although the language of the framework will not stop cyber-breaches in and of itself, it serves as a useful starting point.
[236] *Id. See also* Baer & Sharma, *supra* note 167 (making the point that legislative language must be common "because a poorly-written law could create unintended consequences").

consumer or company from malicious activity. Users must turn knowledge into action, perpetually reeducating themselves on cyber hygiene principles, studying emerging threats, and applying effective countermeasures intended to correct system vulnerabilities. Cyber hygiene is "a means to appropriately protect and maintain IT systems and devices and [to] implement cybersecurity best practices."[237]

Congress should authorize the FTC, the CFPB, and the newly-established Information Security Agency to commence a concerted public awareness campaign within the credit reporting industry, intended to educate company officials and consumers alike on cyber hygiene and information security practices. The campaign should be updated whenever necessary to account for the ever-evolving spectrum of cyber threats. Basic introductory topics for individual consumers should include password management, patches and updates, and multi-factor authentication.[238] More advanced audiences, like corporate information technology specialists, should receive tailored training on various topics to address their sector-specific needs. Subjects should include inventorying hardware and software on company networks, establishing network security and monitoring, disabling vulnerable applications that are not in use, and limiting the number of users with administrative privileges.[239]

F. Recommendation #6 – Utilize Third-Party Penetration Testers

[237] *Importance of Cyber Hygiene in Cyberspace*, INFORMATION SECURITY INSTITUTE, http://resources.infosecinstitute.com/the-importance-of-cyber-hygiene-in-cyberspace/; *see also Good Cyber. Hygiene*, NORTON https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html.

[238] *See also* Brian Krebs, *The Equifax Breach: What You Should Know*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/the-equifax-breach-what-you-should-know/. Paul Szoldra, *A Hacker Told me How to Make a Super Strong Password I Can Actually Remember*, BUS. INSIDER (Apr. 29, 2016), http://www.businessinsider.com/hacker-strong-password-2016-4; NIST, *Back to Basics: Multi-factor Authentication*, NIST (Nov. 22, 2016), https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication. This information is certainly not just limited to companies. While the focus of this essay has been on a large financial corporation, individual citizens need to stay vigilant with their own personal information. Brian Krebs, a blogger and reporter who follows cybersecurity provides helpful guidance for potentially-impacted consumers.

[239] *See also Practice These 10 Basic Cyber Hygiene Tips for Risk Mitigation*, SENTINEL ONE (May 4, 2017), https://www.sentinelone.com/blog/practice-these-10-basic-cyber-hygiene-tips-for-risk-mitigation/.

The newly-created Information Security Agency should manage a team of third-party penetration testers, conventionally known as ethical hackers, to carry out security system checks at the behest of corporate officials. These teams should also include embedded regulators and compliance experts charged with inspecting corporate information security programs.

Hackers are generally regarded as cybercriminals, exploiting loopholes in systems to steal money, cause data destruction, or hold a network hostage from its rightful users.[240] A newer movement, however, utilizes "ethical hackers … hired to help organizations identify and fix security flaws in their systems."[241] U.S. companies are rightfully skeptical, since this involves inviting third-party testers to discover critical flaws in their systems.[242] In the context of the Equifax hack, however, ethical hackers, or "white hat hackers" as they are more commonly known, could have provided the company with an added measure of cyber diligence prior to the data breach, effectively testing Equifax's online dispute portal for recognized vulnerabilities.[243]

The Information Security Agency should employ a team of ethical hackers to conduct penetration testing in the field when requested by a private corporation. This team can identify perceived vulnerabilities in current systems and provide recommendations to resolve critical security flaws. In requesting an external review by a team of white hat hackers, a company like Equifax can demonstrate to consumers that it is exercising due diligence in protecting their sensitive data. Moreover, should a breach actually occur after the team has examined a particular system, the company could potentially lessen its liability by demonstrating that it was in

[240] *See* Hathaway & Crootof, *supra* note 95 at 830; Aimee Chanthadavong, *Ethical Hackers: How Hiring White Hats Can Help Defend Your Organization Against the Bad Guys*, TECHREPUBLIC (June 20, 2016, 4:00 am), https://www.techrepublic.com/article/ethical-hackers-how-hiring-white-hats-can-help-defend-your-organisation-against-the-bad-guys/.
[241] Chanthadavong, *supra* note 240.
[242] *Id*.
[243] *See* Ido Kilovaty, *The Equifax Aftermath - We Need More Hacking*, LAWFARE BLOG (Oct. 6, 2017), https://www.lawfareblog.com/equifax-aftermath-%E2%80%93-we-need-more-hacking (offering a concise description of ethical hackers as cyber intruders who seek "to help secure systems by identifying security vulnerabilities before they can be exploited," thereby helping to uncover a host of vulnerabilities).

compliance with the requisite standard of cyber care. Ideally, the results of this penetration testing should be shared publicly after a company has been given a chance to implement the necessary recommendations. This practice would provide consumers with added reassurance that they are working with a trusted broker. It could also serve as a warning to others in the industry that they must remain vigilant and perpetually educate themselves on emerging cyber threats.

Of course, third-party penetration testers should be heavily regulated so as not to have team members exploiting a company's known vulnerabilities for potential gain. Some important steps have already been taken in the immediate aftermath of the Equifax breach that are helping to move the oversight model closer to such reforms. Specifically, in response to the Equifax hack, the former Director of the CFPB stated in September 2017 that all credit reporting agencies "are going to be getting embedded regulators to ensure that similar breaches of private information don't happen again."[244] Whether this important change actually occurs, this article asserts that embedded regulators and ethical hackers could bring necessary stability to an industry currently in a state of flux.[245]

G. Recommendation #7 - Employ Chief Information Security Officers

All credit reporting agencies should be required to employ a Chief Information Security Officer specifically tasked with monitoring data and information security programs and practices. This Chief Information Security Officer should have open lines of communication with representatives at the Federal Trade Commission, the Consumer Financial Protection Bureau, and the newly-created Information Security Agency.

Equifax employed both a Chief Information Officer and a Chief Security Officer prior to the data breach, both of whom announced their retirement on September 15th, 2017, one week

[244] Jeff Cox, *Big Changes Coming for Credit Firms in Wake of Equifax Hack, CFPB Director Says*, CNBC (Sept. 27, 2017), https://www.cnbc.com/2017/09/27/big-changes-coming-for-credit-firms-in-wake-of-equifax-hack-cfpb-director-says.html.
[245] *See* Harrington, *supra* note 229.

after the hack was first revealed to the public.[246] As a private corporation, Equifax is free to structure its organization however it sees fit, with the current chain of command outlining the internal duties of both the Chief Information Officer and the Chief Security Officer. Nonetheless, the forced retirement of these two individuals raises some important questions. It is plausible that while each of these officers prioritized *either* information *or* security as a part of their daily duties, neither of them were given direct responsibility for the *combined* task of overseeing information *and* security.

As a best practice, all corporations, big and small, should employ a Chief Information Security Officer.[247] That officer should be tasked with monitoring and securing the information in the company's possession.[248] They should be responsible for protecting the PII of consumers and overseeing a robust information security program.[249] Emphasis should also be placed on thwarting hacking attempts, data security compliance, and protecting the privacy of individuals.[250] Additionally, existing security programs should be continuously updated through ongoing risk assessments and internal testing.[251]

Chief Information Security Officers should have a direct line of communication with all other chief officers in a particular corporation and should not face punishment or recrimination

[246] *See* Jennifer Surane, *Equifax Says CIO, Chief Security Officer to Exit After Hack*, BLOOMBERG (Sept. 15, 2017), https://www.bloomberg.com/news/articles/2017-09-15/equifax-says-cio-chief-security-officer-to-leave-after-breachEquifax (revealing that Equifax has since restructured some of their chief positions, and now their chief security officer reports to the chief information officer).
[247] *See also* Baer & Sharma, *supra* note 167 (arguing for a common sense solution in which "[t]he CEO needs to be connected to the IT department, and the IT department needs to be accountable to the general counsel, and to the Board. We need to define and prioritize corporate cyber strategy, not just IT.").
[248] *Id*.
[249] *Id.*; *see also* Safeguards Rule, 16 C.F.R. § 314 (2002).
[250] *See* Alison DeNisco Rayome, *Want to Improve Cybersecurity? Try Phishing Your Own Employees*, TECHREPUBLIC (Aug. 21, 2017), https://www.techrepublic.com/article/want-to-improve-cybersecurity-try-phishing-your-own-employees/.
[251] 16 C.F.R. § 314.4.

for reporting perceived deficiencies in current company practice.[252] They should supervise a team of highly trained professionals charged with combating the ever-changing spectrum of cyber threats. Notably, these individuals must possess the requisite subject matter expertise needed to design and implement a multilayered defense against malicious actors.[253] Large central databases should also be compartmentalized to the greatest extent possible, so that a single security flaw, or single point of failure, does not result in the loss of a veritable treasure trove of information.[254]

More importantly, each respective Chief Information Security Officer should have a direct line of communication with officials at the FTC, CFPB, and newly-created Information Security Agency. They should be made aware of all reporting requirements that arise from legislation, including those related to reporting ongoing security crises and victim notification procedures. These corporate officials should be incentivized to work with government agencies, resulting in increased public-private cooperation and the establishment of a compliance model that is both scalable and adaptable to multiple industries.

VII. CONCLUSION

We are at the beginning of a long struggle, one that requires us to use every resource at our disposal to protect against malicious cybercriminals and hostile nation states.[255] The stakes are unusually high, guaranteeing that the outcome of this great conflict will be felt for

[252] *See* Angeline G. Chen, *In-House Counsel*, *in* RHODES & LITT, *supra* note 136, at 240. As Angeline Chen notes, the parties that need to legally be informed in the event of a breach may not be limited to your own company. Depending on the scope of the security breach, law enforcement (Department of Homeland Security, the Federal Bureau of Investigation, or U.S. Attorney) may also need to be notified may need to be notified.
[253] Bernard & Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, *supra* note 35.
[254] *Id.*
[255] Carlin, *supra* note 11, at 435.

generations.[256] The events surrounding the Equifax hack underscore that our country is in dire need of a comprehensive proposal for reform. To preserve our national security, we must develop a solution that incorporates measures designed to turn our current reactive stance on cybersecurity into an active model of cyber defense.

Notably, the fallout from the Equifax hack is ongoing. In February 2018, corporate officials disclosed to Congress that the breach was far worse than originally thought, with cyber actors having gained access to a host of additional consumer information.[257] While the breach could have a significant effect on individual consumers, exposing them to future credit card fraud and identity theft, its national security implications are unprecedented. The damage inflicted by the Equifax hack can never be undone, with untold potential for foreign powers "to blackmail, shame, or otherwise coerce public officials."[258] Such actions would have profound consequences for our economy and public welfare, thereby influencing our overall national security.[259]

This article's central purpose is to outline a bipartisan vehicle for change. Its recommendations serve as a blueprint for widespread, whole-of-government reform. Just as the 9/11 Commission recommended that Americans achieve unity of effort following the attacks of September 11, 2001, this article endeavors to apply similar mechanisms in our continuing struggle against pervasive cyber threats. Thus, improvements within the credit reporting industry represent an important first step to increased data security. If successful, they signify the U.S.

[256] *Id.*; *see also* Wehbé, *supra* note 108, at 86; Bernard & Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, *supra* note 46.
[257] *Driver's License, Credit Card Numbers: The Equifax Hack Is Way Worse Than Consumers Knew*, USA TODAY (Feb. 10, 2018), https://www.cnbc.com/2018/02/12/the-equifax-hack-is-way-worse-than-consumers-knew.html.
[258] Wehbé, *supra* note 108, at 86.
[259] *See generally* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY, *supra* note 17.

government's renewed commitment to protecting its data, and the data of its private citizens, from malicious foreign adversaries.

Appendix I

DETAILED TIMELINE OF MAJOR EVENTS

Date	Description	Days until next event
March 7, 2017	The Department of Homeland Security notifies Equifax of a critical security flaw, for which a patch is available the same day. Equifax identifies this date as when it first became aware of the vulnerability.	67 days
May 13, 2017	Forensic information leads Equifax to believe that this was the first instance of "unauthorized access to certain files containing personal information."	77 days
July 29, 2017	Equifax security notices suspicious network traffic on its online dispute portal application. It is at this stage that "the Security team investigated and blocked the suspicious traffic that was identified."	4 days
August 2, 2017	Equifax contracts with an independent cybersecurity firm known as Mandiant "to assist in conducting a privileged, comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted."	20 days
August 22, 2017	Equifax registers the domain name www.equifaxsecurity2017.com, which would later be used as their support website for potentially impacted consumers.	16 days
September 7, 2017	Equifax notifies the public of the extent of the breach, and rolls out the website to those impacted.	**Total:** 184 days*

* from the time the security flaw was known until the public was properly alerted.

Appendix II

COMPARISON CHART OF RELEVANT INVESTIGATIVE AUTHORITIES

Federal Trade Commission	(New) **Information Security Agency**	**Consumer Financial Protection Bureau**
- Primarily a financial law enforcement body - Focuses on targeting bad financial practices within private corporations - Prevents fraudulent, deceptive, and unfair business practices - Manages a consumer complaint database that includes more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad - Created by the Federal Trade Commission Act - NOT focused exclusively on data security	- Created out of comprehensive legislation with input from a newly-created bipartisan commission - Combines law enforcement and consumer protection, with specific emphasis on long-term effects on national security - Sets minimum standards for cybersecurity best practices across various industries - Provides incentives for disclosure of breaches and compliance with regulations - Produces recurring reports on cyber hygiene for consumers and businesses alike - Manages a team of third-party penetration testers, a.k.a. "ethical hackers" - Maintains clear oversight and reporting mechanisms with Congress - Establishes an effective communication chain with companies via their Chief Information Security Officers - Focused exclusively on data security	- Helps consumer finance markets function by making rules more effective - Focuses on empowering consumers - Works to consistently and fairly enforce rules across the industry - Tries to return money to consumers who have been unfairly taken advantage of - Facilitates consumer education of industry practices - Created by Dodd-Frank Wall Street Reform Act - NOT focused exclusively on data security

Appendix III

PROPOSED ORGANIZATIONAL CHART FOR THE INFORMATION SECURITY AGENCY