RETHINKING THE FTC'S ROLE AND ABILITIES IN PROTECTING CONSUMER DATA IN THE WAKE OF THE EQUIFAX BREACH

INTRODUCTION

In 2017, Equifax, one of the three largest consumer credit reporting agencies, announced that it had a data breach that exposed roughly 145 million U.S. consumer's Social Security numbers, birth dates, addresses, and driver's license numbers.[1] Yahoo!'s announcement followed shortly, disclosing that its data breach actually compromised sensitive personal information of three billion Yahoo accounts.[2] The repercussions of these data breaches and identity thefts may appear to be an invisible crime, but the impact on the victims is all too real.[3] Injuries from identity theft can range from lifelong financial woes stemming from ruined credit, to denial of much needed welfare or tax refunds, to raised auto insurance rates, to an overwhelming emotional toll on some victims.[4] Nonetheless, consumers

1. *Equifax Announces Cybersecurity Incident Involving Consumer Information,* EQUIFAX (Sept. 07, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628; *see also* Ron Lieber, *How to Protect Yourself After the Equifax Breach*, N.Y. TIMES (Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

2. *See* Selena Larson, *Every Single Yahoo Account Was Hacked - 3 Billion in All*, CNN BUS. (Oct. 4, 2017, 6:36 AM), http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html; *Marissa Mayer Says Yahoo Still Doesn't Know Who Was Behind Web's Biggest Breach*, USA TODAY (Nov. 8, 2017, 2:56 PM), https://www.usatoday.com/story/tech/news/2017/11/08/marissa-mayer-says-yahoo-still-doesnt-know-who-behind-webs-biggest-breach/844716001/ (noting that "[t]he stolen account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers.").

3. *A Lasting Impact: The Emotional Toll of Identity Theft*, EQUIFAX (Feb. 2015), https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf [hereinafter *A Lasting Impact*]. Before the massive breach by Equifax, they released a guide for their many customers to use if their sensitive data is stolen. It is even more relevant because Equifax itself is now the cause of the breach and the harm to consumers.

4. *Id.*; *see also* Jocelyn Baird, *4 Ways Identity Theft Can Impact Your Life*, NEXT ADVISOR BLOG (Nov. 7, 2016), https://www.nextadvisor.com/blog/2016/11/07/x-ways-identity-theft-can-impact-your-life/; Bob Sullivan, *9 Surprising Ways Identity Theft Can Hurt You*, CREDIT.COM

that are impacted by data breaches most probably believe that it is an invisible crime, as courts generally dismiss claims brought against businesses over identity theft from data breaches because of the consumer's inability to have standing or an insufficient showing of causation.[5]

In response to the industry's weak self-regulation, the Federal Trade Commission ("Commission") decided to take the lead in prosecuting businesses for data breaches by "expand[ing] enforcement of existing laws [and not by] pursu[ing] new legislation."[6] Despite several other agencies and supplemental Congressional bills, the Commission is still the primary regulatory body that responds to data breaches.[7] The Commission exceeded its authority in pursuing businesses who suffered a data breach by bypassing the FTC Act's requirement of showing a substantial injury to consumers.[8] The problem is not necessarily that the Commission is regulating these businesses, but rather that it requires a legislative bill to properly expand its regulatory ability and to further give the Commission a more proactive role in data security.[9]

The Commission's response to the industries lackluster self-regulation was the pursuit of enforcement through a broader interpretation of the unfair or deceptive practices or acts clause in section 5(a) of the Federal Trade Commission Act.[10] The reinterpretation allowed the Commission to pursue businesses that failed to adopt "reasonable and appropriate security to protect personal information."[11] It seems like an out of place interpretation, given section 5(a)'s normal usage is against activities related

---

BLOG (June 13, 2014), https://blog.credit.com/2014/06/surprising-ways-identity-theft-can-hurt-you-85080/.

5. *See, e.g.*, Duqum v. Scottrade Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *8 (E.D. Mo. July 12, 2016); Key v. DSW Inc., 454 F. Supp. 2d 684, 689-90 (S.D. Ohio 2006); *see also* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 19, 36 (D.C. Cir. 2017) (demonstrating the dismissal of a consumer complaint because consumers were unable to show that the data breach constituted a concrete injury to warrant Article III standing). .

6. Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 130-31 (2008).

7. FED. TRADE COMM'N, FTC RELEASES ANNUAL PRIVACY AND DATA SECURITY UPDATE (2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-releases-annual-privacy-data-security-update; *see also* Brief for Appellee at 30-32, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015) (No. 14-3514).

8. *See infra* Part II and Part III.

9. *See infra* Part III.

10. Federal Trade Commission Act § 5; 15 U.S.C. § 45(a)(1) (2006); *see also infra* Part I and Part II.

11. Complaint at 3, GMR Transcription Servs. Inc., 2014 WL 4252393 (F.T.C. Aug. 14, 2014) (No. C-4482).

to advertising, marketing, and the sale of products or services.[12] Still, the greater flaw in the Commission's self-extended enforcement power is that in their controlling legislation, section 5(n), requires the Commission to show that the unfair practice will cause "or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves."[13] However, when the Commission brings an action against a business, the complaint is instead focused on whether or not a breach occurred, and often fails to establish or address whether there was a consumer injury.[14]

The main reason the Commission avoids the argument over proving an injury is that it is incredibly difficult to prove that one exposure of a consumer's data led to an injury, evident in the quick dismissal of a majority of consumer complaints.[15] The Commission contends that it is arguing under a different standard than individuals,[16] but the Commission has continually been able to bypass this requirement because a majority of the time data breach cases are quickly settled out of court.[17]

This advantage of avoiding the argument of establishing an injury is rapidly disappearing, as the U.S. Court of Appeals, Eleventh Circuit ruled on June 6, 2018 that the Commission must now show that the standards of unfairness it enforces must be in "'clear and well-established' policies that are expressed in the Constitution, statutes, or the common law."[18] This is troublesome for the Commission, as it must now plead more than that an injury occurred, but that the injury complies with the elements of a legal principle, such as a cause of action for negligence.[19] The Commission most likely may no longer simply state an injury and expect it to be sufficient.

The ruling in Eleventh Circuit, coupled with the overall ineffectiveness of data protection with the massive data breach of sensitive permanent

---

12. FED. TRADE COMM'N, DOT COM DISCLOSURES: INFORMATION ABOUT ONLINE ADVERTISING 3 (May 2000), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf.

13. Federal Trade Commission Act § 5; 15 U.S.C. § 45(n) (2006).

14. *See In re* Twitter, Inc., No. 90-348, 2011 WL 914034 (F.T.C. Mar. 2, 2011) (arguing a section 5 violation without any mention of an injury or possible injury); *see also In re* Uber Tech., Inc., No. 152-3054, 2017 WL 3621179 (F.T.C. Aug. 15, 2017) (finding a section 5 violation without an injury); *In re* Lenovo, Inc., No. 152- 3134, 2017 WL 4021827 (F.T.C. Sept. 5, 2017) (proclaiming that there was a substantial consumer injury without an explanation of the injury or the possible injury).

15. *See Lenovo*, 2017 WL 4021827; *Duqum*, 2016 WL 3683001, at *8; *Key*, 454 F. Supp. 2d at 689-90.

16. *See* Brief for Appellee, *supra* note 7, at 60-61.

17. Scott, *supra* note 6, at 143.

18. LabMD, Inc. v. FTC, 894 F.3d 1221, 1231 (11th Cir. 2018).

19. *Id.*

information by Equifax, illustrate that a new approach to address the growing number of data breaches is needed.[20] Enactment of a legislative bill such as H.R. 3896 to create national standards, increased responsibility, and accountability for businesses and the Commission would be a step in the right direction.[21] H.R. 3896, with the addition of the proposed amendments in Part III seek to empower the Commission to not only prosecute after the fact, but to prevent data breaches from happening in the first place by establishing actual disincentives for violating businesses and through the creation of maintaining a set of national standards for all businesses to adhere to.[22]

This Note argues that the Commission has exceeded its current authority by prosecuting businesses without showing a substantial injury to consumers and requires a new legislative bill to grant the Commission the needed authority to protect the privacy of consumer's data. Part I explains how the Commission empowered itself through the *Chevron*[23] reinterpretation of section 5(a) to pursue businesses whose online business practices exposed consumers online data.[24] Part II will argue that the Commission has extended its general consumer protection powers too far because the Commission fails to satisfy section 5(n)'s requirement of substantial or likely substantial injury to consumers and pursuing actions under section 5(a) instead of creating national standards further harms consumers.[25] Part III argues that if Congressional bill H.R. 3896 is passed, with the addition of several stronger provisions borrowed from the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), it will bring greater protection to consumers from the threats of data breaches.[26] This Note will conclude that as more and more people move their lives online and data breaches affect more Americans than ever, Congress will need to enact legislation to protect the sensitive data held in trust by businesses.[27] Therefore, new responsibilities for businesses and the

20. *Id.* at 1230-31.

21. *See* Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (2017); *infra* Part III.

22. *See* 15 U.S.C. § 45; *infra* Part III.

23. Chevron, U.S.A. v. Nat. Resources Def. Council, 467 U.S. 837 (1984).

24. *See* 15 U.S.C. § 45; *infra* Part I.

25. *See* 15 U.S.C. § 45; *infra* Part II.

26. H.R. 3896; U.S. DEP'T OF HEALTH AND HUM. SERV., SUMMARY OF THE HIPAA SECURITY RULE, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (2013).

27. *See* Simon Kemp, *The Incredible Growth of the Internet Over the Past Five Years Explained in Detail*, THE NEXT WEB (Mar. 2017), https://thenextweb.com/insider/2017/03/06/the-incredible-growth-of-the-internet-over-the-past-five-years-explained-in-detail/ (stating that

Commission to maintain a higher level of data to protect consumers from the harms of these data breaches are needed.[28]

I. THE COMMISSION'S DISCRETION IN DATA BREACH INCIDENTS

A. The Chevron Deference

Under Article 1, section 1 of the U.S. Constitution, Congress is able to create agencies with a statute that lays out the breadth of regulatory power and the purpose of the agency.[29] Congress delegates to agencies both the objective to enforce the text of the agency's controlling statute, and rulemaking abilities.[30] The courts are obligated to abide by the rules or interpretations of rules made by these agencies "unless they are arbitrary, capricious, or contrary to the statute."[31] However, in the seminal case of *Chevron, U.S.A., Inc. v. Natural Resources Defense Council*, the Environmental Protection Agency's interpretation of Congress amended Clean Air Act trumped judicial interpretation of the statute, and granted agencies clout over interpretation of controlling statutes if it is reasonable.[32]

1. Direct Congressional Guidance

The expanded deference to agencies' discretion is not without its limits.[33] The deference given under judicial review to accept an agency's interpretation of statute would be cast aside if Congress "directly spoke[] to the precise question at issue."[34] The question then turns on whether the agency's interpretation is "based on a permissible construction of the

"[i]nternet users have grown by 82%, or almost 1.7 billion people, since January 2012."); *see also infra* Part III.

28. *See infra* Part II.

29. U.S. CONST. art. I, § 1; *see* Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, 98 CORNELL L. REV. 769, 779 (2013).

30. *See* Eric R. Womack, *Into the Third Era of Administrative Law: An Empirical Study of the Supreme Court's Retreat from* Chevron *Principles in* United States v. Mead, 107 DICK. L. REV. 289, 290 (2002).

31. Lauren E. Baer & William N. Eskridge, Jr., *The Continuum of Deference: Supreme Court Treatment of Agency Statutory Interpretations from* Chevron *to* Hamdan, 96 GEO. L. J. 1083, 1086 (2008).

32. 467 U.S. 837, 845, 851 (1984) (finding that the EPA's bubble concept policy was a reasonable interpretation of the Clean Air Act and Congress's intent in the EPA finding the balance between the environment and economic interests).

33. 15 U.S.C. § 45 (2006).

34. *Chevron*, 467 U.S. at 842.

statute."[35] Permissibility depends on the holistic reading of the statute and its accompanying legislative history.[36]

Although this generally can be seen as a restriction of an agency's power, it is more of a restriction on the agency's ability to make rules itself.[37] Congressional guidance can actually expand an agency's power because the question turns from whether the agency can reach this interpretation on a reasonableness test to whether Congress's act allowed an agency to do this action.[38] Therefore, the agency may be granted broader power than if it was using its own discretion to enact their own rules, or interpretation of a statute.[39]

2. Agency's Power with Congressional Silence

When Congress is silent on the issue that falls under the regulatory area of an agency, the agency is then given deference for its interpretation of a statute.[40] The main reason a court will defer to an agency is that agencies are purported to be experts in the field, whereas judges are not.[41] Or as Justice Stevens stated during the discussion of *Chevron*, "[w]hen I am so confused, I go with the agency."[42]

B. The Commission's Extension of Section 5 Under Congressional Silence

The advent of widespread internet commerce occurred nearly eighty years after the FTC Act, but through deference afforded under *Chevron*, the Commission had the ability to respond to this new area of commerce.[43] At first, the Commission insisted that self-regulation and a hands-off approach was the best route, as it was the least intrusive and most efficient means to tackle security issues.[44] By 2000, the Commission felt that businesses did not sufficiently pursue self-regulation and in response to growing privacy concerns, prepared new legislation for Congress to pass to allow the

35. *Id.* at 843.

36. Baer & Eskridge, *supra* note 31, at 1091.

37. *Id.* at 1123-24.

38. *See* Evan J. Criddle, Chevron*'s Consensus*, 88 B.U. L. REV. 1271, 1273-75 (2008).

39. *See* Dudley D. Mccalla, *Deference (And Related Issues)*, 14 TEX. TECH. ADMIN. L. J. 363, 367-70 (2013).

40. *Id.* at 371; *Chevron*, 467 U.S. at 842-43.

41. Criddle, *supra* note 38, at 1274-75; Mccalla, *supra* note 39, at 382.

42. Baer & Eskridge, *supra* note 31, at 1086.

43. *Chevron*, 467 U.S. at 863-64; FED. TRADE COMM'N, *Our History*, https://www.ftc.gov/about-ftc/our-history (last visited Oct. 21, 2017); *see also* Brenda R. Sharton & Jared D. Wilcoxson, *Privacy: The Next Frontier In Online Regulation?*, 45 BOS. B. J. 10 (2001).

44. Scott, *supra* note 6, at 130.

Commission to issue and enforce specific privacy regulations for children.[45] The Commission did not seek to extend protection to consumers in general, because, at the behest of industry leaders, the Commission still felt that the industry was better served by "implementing broad-based and effective self-regulatory programs."[46] However, newly elected President Bush replaced the Commission chairman who sought the proper legislative approach and therefore, eliminated any attempt for a comprehensive expansion of online privacy for consumers.[47] The newly selected Commission chairman instead directed the Commission towards online security protection through a new interpretation of section 5(a)'s unfair or deceptive business practice or act provision to include improper data protection.[48]

Section 5(a) of the FTC Act grants the Commission discretion to prevent all "unfair . . . acts or practices in or affecting commerce."[49] The section is void of enumerated unfair business practices and was most likely drafted in this manner to give the Commission the "sweep and flexibility"[50] needed to respond to "a flexible concept with evolving content."[51] Congress was purposefully silent when drafting, because any attempt at a comprehensive list would have "been incomplete and likely would have become outdated or left loopholes susceptible to easy evasion."[52] The Commission agreed with this sentiment when responding to data breach violations and decided not to create a list with its rule making power, but to proceed on a case-by-case basis analysis of section 5(a) data breach violations to remain dynamic.[53] The Commission chose this method

45. *Id.* at 130-32; MARTHA K. LANDESBERG & LAURA MAZZARELLA, FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 1 (July 1999), https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf.

46. LANDESBERG & MAZZARELLA, *supra* note 45, at 1.

47. *See* TIMOTHY J. MURIS, FED. TRADE COMM'N, PROTECTING CONSUMERS' PRIVACY: 2002 AND BEYOND (Oct. 4, 2001), https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond.

48. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litg., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); Geocities, No. 9823015, 1998 WL 473217, at *13 (F.T.C. Jan. 1, 1998).

49. 15 U.S.C. § 45(a)(1) (2006).

50. FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 241 (1972).

51. FTC v. Bunte Bros., 312 U.S. 349, 353 (1941).

52. JOSHUA D. WRIGHT, FED. TRADE COMM'N, SECTION 5 RECAST: DEFINING THE FEDERAL TRADE COMMISSION'S UNFAIR METHODS OF COMPETITION AUTHORITY 2 (June 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/section-5-recast-defining-federal-trade-commissions-unfair-methods-competition-authority/130619section5recast.pdf.

53. *Id.*

because "[y]ou don't do the rulemaking cause you can't anticipate the problems until they occur."[54]

In turn, the public has been left in the dark over which standards apply and what level of data security is reasonable under Commission standards.[55] The lack of rulemaking has allowed the Commission flexibility, but also free reign by not articulating the scope of its power.[56] However, the Commission's method of using its afforded deference to pursue data breach violations does have its limits in the form of section 5(n)'s requirement for the Commission to show a substantial or likely injury from the act or practice.[57]

II. LACK OF SUBSTANTIAL HARM

Congress's relative silence in regard to data breaches has allowed the Commission to continue pursuing data breach violations through section 5 of the FTC Act's general consumer protection clause, both out of necessity and because of the much needed ability to dynamically respond to data breaches.[58] Section 5's general consumer protection clause is essentially a catch-all provision that allows the Commission to respond to practically any form of unfair competition, but is tempered with Congress's original intention of the FTC Act to allow businesses to freely transact with one another without the concern of unfair practices.[59] There is a caveat in using section 5(a)'s general consumer protection clause, as any complaint brought

54. Angelique Carson, *LabMD Argues 'Matter of Principle' in FTC Data-Security Appeal*, INT'L ASS'N OF PRIVACY PROF'L:THE PRIVACY ADVISOR (June 26, 2017), https://iapp.org/news/a/11th-circuit-hears-arguments-in-labmd-v-ftc-appeal (noting that the judge presiding over the appeal of *LabMD v. FTC* commented on why the FTC's argument that they do not do rule making for data security violations because of the nature of security or privacy violations are dynamic and that it is "entitled" to regulate on a case-by-case basis).

55. *Id.*

56. *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement*, 24 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CA. 229, 236 (2015) (explaining that the FTC chooses not to make rules because flexibility to counter technological advancements in data security is better than issues standards to guide businesses compliance).

57. Jennifer Woods, *Federal Trade Commission's Privacy and Data Security Enforcement Under Section 5*, A.B.A. (Mar. 2013), https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/federal_trade_commissions_privacy.html.

58. Alden Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, THE HERITAGE FOUND. (Sept. 10, 2014), http://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator; Merritt Baer & Chinmayi Sharma, *What Cybersecurity Standard Will a Judge Use in Equifax Breach Suits*, LAWFARE (Oct. 20, 2017, 7:30 AM), https://www.lawfareblog.com/what-cybersecurity-standard-will-judge-use-equifax-breach-suits.

59. *See* David L. Belt, *The Standard for Determining "Unfair Acts Or Practices" Under State Unfair Trade Practices Acts*, 80 CONN. B. J. 247, 253-55 (2006); Woods, *supra* note 57.

forward must comply with section 5(n) of the FTC Act, which demands that the Commission prove that the act or practice "causes or is likely to cause substantial injury to consumers."[60] The precedence set in *International Harvester Co.*, requires an injury shown by the Commission to not be "trivial or merely speculative harms," and that the "injury must be substantial."[61] The injury from *International Harvester* was substantial, as it involved a health and safety risk of severely hot fuel being shot in the air from the tractor's fuel tank.[62] However, when the Commission files complaints for data breach violations, it has continually left out the argument that consumers have faced any injury.[63]

A. The Difficulty of Showing Injuries from Data Breaches

The Commission avoids arguing that the consumers have incurred a substantial injury for the simple reason that it is extremely difficult for consumers themselves to prove any sort of injury because of data breaches.[64] In order for consumers to make it past the Article III standing requirement, they must allege, among other requirements, that the data breach inflicted a "concrete, particularized injury on them," and that the company who mishandled their information caused the injury.[65] Any argument brought forward by consumers usually rests upon a speculative harm, which courts consider to be valueless, as it is "rested on a chain of events that [are] both 'highly attenuated' and 'highly speculative.'"[66] Therefore, courts have routinely held that consumers have not properly pleaded injury in fact by lack of showing an injury and their cases are dismissed.[67]

---

60. 15 U.S.C. § 45(n) (2006).

61. *See* 104 F.T.C. 949, 1073 (1984), 1984 WL 565290 (concerning a non-deceptive failure to disclose the dangers of a Harvester tractors shooting hot fuel into the air, the FTC was allowed to bring a claim under section 5. Also, the court noted that the goal of section 5 was to allow markets to operate freely and fairly and to support informed consumer choice).

62. 104 F.T.C. 949.

63. *Id.*; *see also* Lenovo, Inc., No. 152-3134, 2017 WL 4021827 (F.T.C. Sept. 5, 2017) (proclaiming that there was a substantial consumer injury without an explanation of the injury or the possible injury); Uber Tech., Inc., No. 152-3054, 2017 WL 3621179 (F.T.C. Aug. 15, 2017) (finding a section 5 violation without an injury).

64. *See* Rosado v. eBay Inc., 53 F.Supp.3d 1256, 1265-66 (N.D. Cal. 2014) (finding that the plaintiff failed to suffer an unavoidable economic injury); Mathew J. Schwartz, *Why So Many Data Breach Lawsuits Fail*, BANK INFO SECURITY (May 11, 2015), https://www.bankinfosecurity.com/data-breach-lawsuits-fail-a-8213.

65. Remijas v. Neiman Marcus Grp., 794 F.3d 688, 692 (7th Cir. 2015).

66. *Id.* at 693 (quoting Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).

67. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547-50 (2016).

Unfortunately, consumers actions against businesses who have compromised their data are largely dismissed in the preliminary stages because they are declared to not have an injury.[68] This is not to say that an injury is not present for victims of identity theft.[69] Beyond the time spent getting new credit cards and refunds for fraudulent purchases, identity theft can also have lasting effect throughout your entire life.[70] Besides the financial harms of identity theft, the emotional toll on victims of identity theft is akin to "emotional effects [felt by] victims of violent crimes, ranging from anxiety to emotional volatility."[71] Victims of identity theft can become overwhelmed with both the stress of financial strain and vulnerability associated with this invasive crime.[72] They may also continue to feel "exposed all the time," even during a simple payment transaction at a grocery store where their card is swiped twice.[73]

Nonetheless, a majority of data breach cases are still dismissed by judges over their inability to prove standing under Article III.[74] Simply put, consumers cannot show that a specific injury, as from *International Harvester,* occurred to them was caused by a data breach.[75] It seems at odds with logic that the Commission is able to argue that their complaints are based on substantial injury when consumers cannot even prove an injury.

Furthermore, businesses are now turning to the dismissal of consumer cases based on direct causation by showing that the injury was "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court."[76] This is an effective strategy to take, as it may be difficult if not nearly impossible for a consumer to directly tie the fraudulent usage of their sensitive data to

---

68. *See Rosado*, 53 F. Supp. 3d at 1266 (finding that the plaintiff failed to suffer an unavoidable economic injury); Schwartz, *supra* note 64.

69. *A Lasting Impact*, *supra* note 3; *see also* Daniel J. Penofsky, 112 AM. JUR. 1 *Trials* § 39 (2017).

70. *See* Penofsky, *supra* note 69.; Sullivan, *supra* note 4.

71. *A Lasting Impact*, *supra* note 3; *see* Penofsky, *supra* note 69.

72. Herb Weisbaum, *ID Theft Can Take Heavy Emotional Toll on Victims,* TODAY (Nov. 20, 2014, 9:11 AM), https://www.today.com/money/id-theft-can-take-heavy-emotional-toll-victims-1D80305639.

73. *Id.*; *A Lasting Impact*, *supra* note 3.

74. *See* Rosado v. eBay Inc., 53 F. Supp. 3d 1256, 1266 (N.D. Cal. 2014) (finding that the plaintiff failed to suffer an unavoidable economic injury); Schwartz, *supra* note 64.

75. Schwartz, *supra* note 64; *see also* Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984), 1984 WL 565290 ("[FTC] charges that Harvester's gasoline-powered tractors were subject to a phenomenon known as fuel geysering – the forceful ejection of hot fuel through a loosened gas cap. The complaint further charges that fuel geysering could result in serious fires, sometimes involving the tractor operator").

76. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

the data breach.[77] There are trillions of gigabytes worth of information under the control of businesses, coupled with the high probability that consumers willingly give away sensitive information, which makes it extremely difficult to pinpoint one instance.[78] Consumers are not able to bring a case forward because their injuries are speculative and involve non-substantial harms.

B. The Commission's Arguments in Support of its Injury Pleading

This begs the question, how is the Commission able to bring complaints under section 5 when case law states that consumer injuries are too speculative and non-substantial? The Commission may point to the United States Court of Appeals, Ninth Circuit's *FTC v. Neovi, Inc.* opinion.[79] The Ninth Circuit quoted the Commission's own explanation of the limitations on its authority from its letter to Congress that stated "[a]n act or practice can cause 'substantial injury' by doing a 'small harm to a large number of people, or if it raises a significant risk of concrete harm.'"[80] However, the facts of the case are different than the nature of data breaches because it was an actual quantifiable harm.[81] The offending business, Qchex, was an online check service where fraudsters created roughly 13,750 accounts that fraudulently withdrew more than $402,750,000 from innocent bystander's accounts.[82] The situation in *Neovi* is different than data breaches because the damages are not speculative and can be directly attested to Qchex "under a theory of aiding and abetting" the fraudsters.[83]

---

77. *See* Fosters v. Essex Prop., Inc., 2017 WL 264390, at *2 (N.D. Cal. Jan. 20, 2017); David Cohen & Ani-Rae Lovell, *Another Way to Challenge Standing in Data Breach Cases*, LAW 360 (Apr. 24, 2017, 6:30 PM), https://www.law360.com/articles/914711/another-way-to-challenge-standing-in-data-breach-cases.

78. *See* Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Apr. 6, 2018), https://digitalguardian.com/blog/history-data-breaches (noting that as of 2015, there was an estimated 7.9 zettabytes of global data, with 6.23 zettabytes being managed by enterprises); Steve Olenski, *For Consumers, Data Is A Matter of Trust*, FORBES (Apr. 18, 2016, 9:35 AM), https://www.forbes.com/sites/steveolenski/2016/04/18/for-consumers-data-is-a-matter-of-trust/#6ecbe1f178b3 (finding that consumers are still likely to give sensitive information to 75% of companies they trust, and 80% to companies that had "special offers or data-enabled benefits").

79. 604 F.3d 1150 (9th Cir. 2010).

80. *See id.* at 1157 (quoting Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985)); Letter from Federal Trade Commission to Senator Ford and Danforth (Dec. 17, 29180), *reprinted in* H.R.Rep. No. 156, Pt.1, 98th Cong., 1st Sess. 33-40 (1983), appended in *Int'l Harvester*, 104 F.T.C. at 1061.

81. *See Neovi*, 604 F.3d at 1154.

82. *Id.*

83. *Id.* at 1157.

The simpler answer is that the Commission has yet to be challenged in court over data security violations and has only had to plead that there is a "plausible case of substantial consumer harm."[84] Of the very few unfairness actions that are challenged, the United States Court of Appeals, Third Circuit ruled in favor of the Commission's over a section 5(a) action in *Federal Trade Commission v. Wyndham Worldwide Corp.*[85]

1. Federal Trade Commission v. Wyndham Worldwide Corp.

Wyndham Worldwide Corp. is a hospitality company whose data base was breached by hackers three times in a span of two years.[86] In the last attack by hackers, they obtained payment card information for roughly 69,000 customers from twenty-eight hotels.[87] Wyndham hotels argued that they themselves cannot treat their customers unfair themselves, if "the business *itself* [was] victimized by criminals."[88] The court quickly dismissed this argument as they provided no authority for this argument but gave support to the Commission bringing data security claims despite not fully pleading a substantial injury to plaintiffs.[89] The court proceeded to state that unfairness claims generally "involve actual or completed harm," but also that the FTC Act "expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[90] Generally, the conduct only needs to be a proximate cause and not the "*most* proximate" cause of an injury to be a foreseeable harm.[91] Wyndham did not contest that the harm was foreseeable, simply for the reason that it would be implausible to argue foreseeability for the second and third breaches.[92] Essentially, *Wyndham* stands for the principle "that conduct can be unfair before actual injury occurs" and not for the principle that the purposed injury is unlikely to occur.[93]

---

84. *See* Brief for FTC at 57, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015) (No. 14-3514).

85. 799 F.3d at 246 (stating the court agreed with the Commission that the "ultimate harm was reasonably foreseeable").

86. *See id.* at 241-42.

87. *Id.*

88. *Id.* at 246.

89. *Id.*

90. *Id.*

91. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 449 (AM. LAW INST. 1965) (stating that even if there is an intervening third party that makes an actor negligent, "whether innocent negligent, intentionally tortious, or criminal, does not prevent the actor from being liable for harm caused thereby").

92. *See Wyndham*, 799 F.3d at 246.

93. Brief of the NTSC as Amicus Curiae in Support of Petitioner and Vacatur at 11, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270).

2. The Commission's Untested Argument of Differing Standards

The Commission argued that itself and consumers are arguing under different standards. It contested that private plaintiffs must show an actual or imminent injury that impacts the consumer in an individual and personal way.[94] Whereas, the Commission argued that it need *only* contend that the business practice causes or is likely to cause an injury to consumers.[95] It further claims that it is immaterial to identify consumers who suffered any injury, only that some consumers suffered an injury because "the nature of the harm is so diffuse[d] that specific identities of the victims would be nearly impossible to ascertain."[96] However, the Commission's argument has not been ruled on directly by courts and this argument has even been completely avoided, as the majority of data breach cases have been resolved by consent orders.[97]

The usual process is that the Commission files a complaint in an administrative proceeding and the business complies via a consent order.[98] Businesses follow this route of not challenging their case and the Commission's authority, in order to mitigate embarrassment and legal fees.[99] This has effectively allowed the Commission to bypass the difficult requirement that consumers face in trying to bring their case forward. That is not the situation now, as the Commission's power to challenge businesses for security breaches under section 5 has significantly changed with *LabMD v. FTC.* [100]

C. LabMD v. Federal Trade Commission

It was not until 2015 that a business decided to argue that the Commission is violating section 45(n) by not showing a substantial injury.[101] Beginning in 2010, the Commission launched an investigation

94. *See* Brief for the FTC at 60, *Wyndham*, 799 F.3d 236 (No. 14-3514).

95. *Id.*

96. *Id.* at 57.

97. *See* Twitter, Inc., 151 F.T.C. 162 (2011), 2011 WL 914034 (Arguing a section 5 violation without any mention of an injury or possible injury); *see also* Lenovo, Inc., No. 152-3134, 2017 WL 4021827 (F.T.C. Sept. 5, 2017) (proclaiming that there was a substantial consumer injury without an explanation of the injury or the possible injury); Uber Tech., Inc., No. 152-3054, 2017 WL 3621179 (F.T.C. Aug. 15, 2017) (finding a section 5 violation without an injury); Woods, *supra* note 57.

98. *Id.*

99. *Id.*; Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued*, 90 FLA. B. J. 30 (2016).

100. Carson, *supra* note 54.

101. LabMD, Inc. v. FTC, 894 F.3d 1221, 1226 (11th Cir. 2018).

into LabMD over a potential data breach of the clinic's patient files.[102] The laboratory held sensitive personal information of over 750,000 patients and included "names, birthdates, addresses, and Social Security numbers, as well as certain medical and insurance information."[103] The Commission filed a complaint and charged LabMD with unreasonable computer data security practices that likely constituted a substantial injury.[104] The proposed injury stemmed from a leak in 2005 caused by a billing manager who used "a peer-to-peer file-sharing program called LimeWire on her work computer."[105] LimeWire allowed other users to search and download any file in the billing manager's computer, which happened to include 1,718 pages of sensitive personal information.[106] The only known entity that downloaded the 1,718 pages was a data security company, Tiversa.[107] Tiversa downloaded the information and used it only as a means of soliciting LabMD to hire them for data protection services, as it was evident they needed additional help in this matter.[108] Although the sensitive information was held by unauthorized hands, how is there a substantial injury to the consumers if the information was never released?[109]

The administrative judge presiding over the complaint found that the Commission's argument of hypothetical harm was an insufficient basis for holding that the breach was likely to cause future harm.[110] The Commission proceeded by reversing the holding and declaring that the administrative law judge improperly applied the FTC Act's standard of unfair business practices.[111] The Commission instead held that the mere fact that the document was disclosed at all constituted a substantial "privacy harm" to the consumers.[112] LabMD appealed this decision to the U.S.

---

102. LabMD, Inc. v. FTC, 678 Fed. App'x 816, 818 (11th Cir. 2016).

103. *Id.*

104. Respondent LabMD, Inc.'s Corrected Proposed Conclusions of Law, LabMD, Inc., No. 9357 (F.T.C. 2015) 2015 WL 4967223, at *1.

105. *LabMD*, 678 Fed. App'x at 818.

106. *LabMD*, 678 Fed. App'x at 818; Respondent LabMD, Inc.'s Corrected Proposed Conclusions of Law, *supra* note 104, at *96..

107. *LabMD*, 678 Fed. App'x. at 819 (finding that "there was no proof anyone other than Tiversa had downloaded the 1718 file").

108. *Id.* at 818.

109. *Id.* at 819 (showing that LabMD is no longer operational, as it has "no employees, and keeps only the records required by law in a secured room, on an unplugged computer that is not connected to the internet").

110. *Id.* at 818-19; Carson, *supra* note 54.

111. *LabMD*, 678 Fed. App'x at 818-19; Respondent LabMD, Inc.'s Corrected Proposed Conclusions of Law, *supra* note 104, at *37 (arguing that as a matter of law the FTC failed to prove by a preponderance of the evidence that LabMD caused an actual or likely harm to competition or consumers through an unfair practice or act); Carson, *supra* note 54.

112. *LabMD*, 678 Fed. App'x at 820.

Court of Appeals for the Eleventh Circuit with its key arguments that the Commission exceeded its authority under section 5 when it found "LabMD's data security practices 'unfair' under section 5" and that the Commission's order of "remedies and relief are invalid even assuming a section 5 violation."[113]

The Eleventh Circuit partially agreed with LabMD and issued a stay of the Commissions' consent decree against LabMD.[114] It observed that there was merit to LabMD's argument and that the Commission's interpretation of section 5 "may not be reasonable."[115] The court agreed with LabMD's argument that the theft of the 1718 file did not have a tangible effect on consumers[116] as the Commission "did not point to any tangible harm to any consumer, because there is no evidence that any consumer suffered a harm such as identity theft or physical harm."[117] The Commission's argument that there was injury was based solely on the disclosure of the 1718 file without authorization from the consumers and that the "consumers suffered a 'privacy harm' that may have affected their reputations or emotions, which therefore constituted a substantial injury."[118] This is in contrast to the Commission's Policy statement that the Commission "is not concerned with . . . merely speculative harms," and that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[119]

The Eleventh Circuit's most recent decision did not decide whether or not the Commission has the authority to bring suits against businesses for data security violations, but rather narrowly tailored their opinion to only concern the Commission's order.[120] The decision still dealt a hard blow to the Commission, as its main method of enforcement was given a substantial hurdle.[121] The court states that the Commission is required to specifically list the remedial actions that need to be accomplished in its cease and desist

113. Brief of Petitioner, LabMD, Inc. at 1, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270).

114. *LabMD*, 894 F.3d at 1227.

115. Brief of Petitioner, LabMD, Inc., *supra* note 113, at *9.

116. *Id.* at *5.

117. *LabMD*, 678 Fed. App'x at 820.

118. *Id.*

119. *Id.*

120. *See* LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018); Alison Frankel, *There's a Big Problem for the FTC Lurking in 11th Circuit's LabMD Data-Security Ruling*, REUTERS (June 7, 2018, 1:26 PM), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

121. Frankel, *supra* note 120 (stating the 11th Circuit's "well-established legal standard" is a substantial hurdle for the Commission).

orders and injunctions.[122] The Commission's order to LabMD contained no prohibitions and commanded LabMD to "meet an indeterminable standard of reasonableness."[123] That was not the only blow to the Commission's enforcement of data security violations, as the Eleventh Circuit also stated that the Commission must satisfy the second 1964 unfairness factor.[124] In 1964, the Commission established three factors to consider when exercising its unfairness authority.[125] The second 1964 unfairness prong required that the "act or practice's 'unfairness' must be grounded in statute [and] judicial decisions."[126] Therefore, the Commission cannot bring an unfairness claim through section 5(a) by arguing that a substantial injury merely occurred but must now properly argue that the violating businesses action satisfied a doctrine such as invasion of an interest of another.[127]

The implications of Eleventh Circuit's opinion over the Commission's power to bring actions under the unfairness doctrine is rather grim. The Commission may still appeal this decision en banc or to the U.S. Supreme Court,[128] but it probably will not, given the evidentiary gaps of the LabMD action.[129] The Eleventh Circuit's opinion severely harmed the Commission's current enforcement method of data security breaches by adding an additional hurdle to the Commission's consent decrees and by stating that the Commission must ground its unfairness claims in legal standards.[130] The Commission may not have the lenience it once had before to bring claims without having to argue its merits at trial, as these new hurdles make it an easier gamble to challenge the Commission's regulatory authority.[131] However, there is a silver lining for consumers, since the Commission has now been forced to reevaluate its method.[132] The best and most effective avenue for the Commission would be to once again pursue a legislative bill to unquestionably grant the Commission's authority over

122. *LabMD*, 894 F.3d at 1236.

123. *Id.*

124. *Id.* at 1228.

125. *Id.*

126. *Id.* at 1229.

127. *Id.* at 1231.

128. Frankel, *supra* note 120.

129. *See* Brief of Petitioner, LabMD, Inc., *supra* note 113, at *4-*5 (showing that the Commission had to fabricate evidence to initially establish that there was an injury).

130. Frankel, *supra* note 120.

131. *Still Waiting on 'LabMD' Ruling on FTC Data Security Power*, BLOOMBERG BNA (Dec. 13, 2017), https://www.bna.com/waiting-labmd-ruling-b73014473153/.

132. *See* Daniel Castro, *LabMD Ruling Gives FTC Chance for Course Correction on Cybersecurity*, MORNING CONSULT (June 13, 2018), https://morningconsult.com/opinions/labmd-ruling-gives-ftc-chance-for-course-correction-on-cybersecurity/.

data breaches, and to also give the Commission a more active role in protecting consumers through the creation of national standards.[133]

D. The Nonexistent Standards of Data Security

With the decision of the Commission to pursue data breaches on a case-by-case approach, the Commission fails to provide a clear data security standard.[134] The Commission contends that the lack of standards is necessary for data security because the nature of harm of data security is *dynamic*.[135] The Commission backs up its argument that it can choose whatever strategy they wish to take, as the Commission is "fully entitled" to take this route given current legislation.[136] Although this is not the worst method to combat data breaches, as security strategies vary greatly depending on the industry or scale of operation, it leaves businesses with no bar to gauge their security protocols or to even have a security protocol at all.

1. A Standard is Needed for Data Security

When the Commission brought a complaint against the married person dating website, Ashley Madison, because of the prior data breach, it was found that the thirty-seven million user website was not adequately protected.[137] This came as a surprise, as the breach and the subsequent posting of Ashley Madison member's information on a searchable database online by the hackers is rather counter intuitive to Ashley Madison's business model for primarily married men to engage in "clandestine

---

133. *A Lasting Impact* , *supra* note 3; Megan Leonhardt, *Equifax Is Going to Make Millions Off Its Own Data Breach*, TIME (Oct. 4, 2017), http://time.com/money/4969163/equifax-hearing-elizabeth-warren-richard-smith/; Jim Puzzanghera, *Senators Slam Equifax for Making Money Off Massive Data Breach and No-bid IRS Contract,* L.A. TIMES (Oct. 4, 2017, 12:40 PM), http://www.latimes.com/business/la-fi-equifax-senate-20171004-story.html; Weisbaum, *supra* note 72.

134. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 254 n.19 (3d Cir. 2015) (finding that the Supreme Court has allowed an agency where a generalized standard framework would be "doubtful," case-by-case analysis is permissible).

135. Carson, *supra* note 54. The judge presiding over the appeal of *LabMD v. FTC* commented on why the FTC's argument that they do not do rule making for data security violations because of the nature of security or privacy violations are dynamic.

136. *Id.*

137. Complaint at 11, FTC v. Ruby Corp., No. 16-cv-02438 (D.C. Dec. 14, 2016); Rene Millman, *Ashley Madison's Source Code Reveals Poor Security Practices,* SC MEDIA (Sept. 9, 2015), https://www.scmagazineuk.com/ashley-madisons-source-code-reveals-poor-security-practices/article/535024/; Sharon D. Nelson & John W. Simek, *Recent High-Profile Data Breaches and Lessons Learned from Them*, 41 MONT. LAW. 16, 19 (2016).

hookups."[138] Hackers were easily able to bypass Ashley Madison's poor security measures, as its security credentials were poorly chosen to be hardcoded, and even encryption keys for the network were stored as a plain text file in emails under the name "shared passwords."[139] This would be akin to leaving all of the passwords to your accounts on a note taped to your computer.

Ashley Madison was not alone regarding insufficient security practices and protection, LabMD had the same problems.[140] However, LabMD's issue was caused by a relatively minor hiccup by a lone employee and relates more to inadequate training than the comprehensive lack of data security by LabMD.[141] Businesses frequently do not elevate data security and training to the level it needs to be, considering the millions of dollars in cost per data breach.[142] A reason for this is that they are not required by the Commission to meet any standard regarding data security.[143] The data security world needs routinely updated security standards to provide a baseline of rules for businesses to follow.[144]

2. The Commission's Choice of Discretion Over a Concrete Standard

The Commission has argued against providing standards for businesses to guide themselves, because the complicated nature of data security requires a dynamic response.[145] Additionally, the original intent behind the

---

138. Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data,* WIRED (Aug. 18, 2015, 5:55 PM), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (showing that the injury caused to consumers was rather major as hackers posted the names of spouses seeking extramarital affairs online on a searchable database for everyone to view).

139. Complaint, *supra* note 137, at 10; Millman, *supra* note 137 (stating that hard coding security credentials fixes one common issue with data security but creates a plethora of other "security implications that is far bigger and with more potential for mis-use").

140. LabMD, Inc. v. FTC, 678 Fed. App'x 816, 818 (11th Cir. 2016).

141. *Id.* (showing that the breach was caused by poor training because the billing manager used a work computer to use a peer-to-peer sharing program).

142. *See* FED. TRADE COMM'N, SMALL BUSINESS COMPUTER SECURITY BASICS (Apr. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/small-business-computer-security-basics; FED. COMMC'NS COMM'N, CYBERSECURITY FOR SMALL BUSINESS, https://www.fcc.gov/general/cybersecurity-small-business; Meghan M. Biro, *Data Security Must Be a Top Priority for HR*, HUFFPOST (July 13, 2016, 1:08 PM), https://www.huffingtonpost.com/meghan-m-biro-/data-security-must-be-a-t_b_10932396.html; *Data Breaches Cost US Businesses an Average of $7 Million Here's the Breakdown*, BUS. INSIDER (Apr. 27, 2017, 11:00 AM), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4.

143. *See* Kathryn F. Russo, *Regulation of Companies' Data Security Practices Under the FTC Act and California Unfair Competition Law*, 23 J. ANTITRUST & UNFAIR COMPETITION L. SEC. ST. B. CA. 201, 204-05 (2014); Abbott, *supra* note 58.

144. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., COMMITMENT TO SERVING CUSTOMERS, https://www.nhtsa.gov/about-nhtsa/nhtsas-core-values.

145. Abbott, *supra* note 58; Baer & Sharma, *supra* note 58.

Commission was to balance regulation with the free flow of commerce and allow businesses to freely transact with one another without the concern of unfair practices.[146] This business friendly objective that is being upheld by the Commission refusing to set solid security standards to promote the free flow of commerce comes at the expense of the consumer.[147] Businesses time and again, from Ashley Madison's lack luster and wholly insufficient security system, to Equifax's poor system procedures, leave online security to the wayside.[148] This is a serious problem that will only get worse when considering not only that the internet and data breaches are both growing in scope and magnitude, but also that Congress has been slow in creating regulatory abilities to match.[149] Furthermore, a lack of national standards creates a free-for-all which can be especially harmful when considering that some businesses may benefit from a data breach.[150] During the Senate Banking Committee's hearing on the 2017 Equifax data breach, as Senator Elizabeth Warren correctly pointed out, Equifax has benefited from the data breach in the form of millions of dollars from its own data breach, as Equifax is concurrently in the business of protecting consumers against fraud from data breaches.[151]

Consumers and businesses are both hurt by the Commission not adapting standards for data security and by the Commission overextending their interpretation of section 5(a).[152] Whether from emotional damage or monetary harm, online privacy of consumers is not being sufficiently protected.[153] The Commission's original plan to let the industry handle data

146. Belt, *supra* note 59, at 253-55.

147. Abbott, *supra* note 58; Baer & Sharma, *supra* note 58; Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds,* NBC NEWS (July 24, 2017, 7:18 AM), https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881.

148. Complaint, *supra* note 137, at 9-12; Nelson & Simek, *supra* note 137; *Equifax Announces Cybersecurity Incident*, *supra* note 1; Lieber, *supra* note 1; Millman, *supra* note 137.

149. Charlie Mitchell, *It's Been One Year After the Equifax Hack Bombshell. So What's Been Done?*, WASH. EXAMINER (Sept. 11, 2018), https://www.washingtonexaminer.com/policy/technology/its-been-one-year-after-the-equifax-hack-bombshell-so-whats-been-done; Weisbaum, *supra* note 147 (showing that although there have been sizable data breaches a decade or so ago from TK/TJ Maxx's 94 million affected and AOL's 92 million affected, there has been a large uptick in number of effective and frequencies of data breaches: Equifax's 143 million affected, River City Media's 1.3 billion affected, Anthem's 80 million affected, Ebay's 145 million affected, Deep Root Analytic's 198 million affected, to Target's 70 million affected)..

150. Castro, *supra* note 132.

151. Leonhardt, *supra* note 133; Puzzanghera, *supra* note 133; Weisbaum, *supra* note 147; *see also* Zack Whittaker, *A Year Later, Equifax Lost Your Data But Faced Little Fallout*, TECH CRUNCH (Sept. 8, 2018), https://techcrunch.com/2018/09/08/equifax-one-year-later-unscathed/.

152. *See supra* Part II.

153. *A Lasting Impact*, *supra* note 3; Leonhardt, *supra* note 133; Puzzanghera, *supra* note 133; Weisbaum, *supra* note 72.

security matters is still lacking, given the crucial nature of the sensitive information and competing aspect of profits and consumer protection.[154] Therefore, Congress must provide legislative guidance not only to the Commission, but also to businesses in how they handle the data security of millions of Americans.[155]

III. THE SOLUTIONS

Congress needs to enact a new bill to outline requirements for data protection, limit the Commission's overreach by proscribing when it can pursue businesses over data breaches, and give the Commission the duty to create national standards for businesses to follow. Many major data breaches over the last few years revolved around businesses having lackluster security measures or practically none to speak of.[156]

The Commission and its current form of enforcement under section 5(a) is inadequate if the agency is only picking up the pieces after a breach.[157] It would be unfair to say that the Commission is entirely inadequate in its handling of data breaches, but rather it is an issue of the Commission needing an update and further expansion of regulatory ability and objectives to combat the issues of data breaches, especially in wake of the Eleventh Circuit's opinion.[158] The Commission's necessary yet unjustified overreach with section 5's general consumer protection claim to regulate businesses regarding data breaches is actually a Congressional issue.[159] Congress is the only entity permitted to not only force the Commission to make rules, but also to concretely give the Commission power to pursue businesses over data breaches and lackluster data security.[160]

The Commission, for better or worse, has done its best to stop data breaches under the at times unreasonable extension of section 5(a), but the

---

154. *See* Leonhardt, *supra* note 133; Puzzanghera, *supra* note 133; *supra* Part I.A.1.

155. *See supra* Part I.

156. *See* LabMD, Inc. v. FTC, 678 Fed. App'x 816, 818 (11th Cir. 2016); Complaint, *supra* note 137, at 9-12; Nelson & Simek, *supra* note 137; Millman, *supra* note 137; Lily H. Newman, *Equifax Officially Has No Excuse,* WIRED (Sept. 14, 2017, 1:27 PM), https://www.wired.com/story/equifax-breach-no-excuse/.

157. *See World's Biggest Data Breaches*, INFO. IS BEAUTIFUL (Jan. 2018), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; Weisbaum, *supra* note 147.

158. *See* David A. Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big For Its Breaches?*, 2011 STAN. TECH. L. REV. 12, 1-8 (2011); *see also supra* Part I.A.1.

159. Zetoony, *supra* note 158, at 5-7; *see also supra* Part I.A.1.

160. *See* Zetoony, *supra* note 158; *supra* Part I.A.1.

time has come for Congress to expand the Commission's oversight with the enactment of a new bill.[161] Congress need only to look to Representative Janice Schakowsky's Secure and Protect American's Data Act, H.R. 3896, to find an appropriate bill for the necessary changes to the Commission's handling of data breaches.[162] H.R. 3896 provides a good baseline for changes to the Commission's approach to data breaches.[163]

A. Secure and Protect Americans' Data Act, H.R. 3896

The proposed bill, H.R. 3896, was created with the goal of requiring "entities who collect and maintain personal information of individuals to secure such information."[164] The bill aims to fulfill this goal by assigning a standard for businesses to adhere to and actively respond to.[165] This may be counterintuitive to many who feel that self-regulation is still the best manner to approach data security, but given the current state of data security, a more active approach is necessary.[166]

The proposed bill lays out a general standard for businesses to establish and maintain their data security system.[167] Businesses would now be given a general standard to adhere to, and also have a duty to keep their data security practices up to date and prepare a process to take "preventive and corrective action to mitigate against any vulnerabilities identified."[168] Once a breach has occurred, the businesses would also be required to provide

---

161. *See supra* Part III.

162. Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (2017); Cory Bennett, *Dem Offers Rival Bill on Data Security*, THE HILL (Nov. 3, 2015, 11:44 AM), http://thehill.com/policy/cybersecurity/258958-house-dem-to-take-another-shot-at-data-security-bill; Howard Feinberg, *House Ready to Draft a Data Security Bill: Commerce Subcommittee Debates Details,* INSIGHTS ASS'N (Jan. 29, 2015), http://www.insightsassociation.org/article/house-ready-draft-data-security-bill-commerce-subcommittee-debates-details; Jennifer Surane, *These Five Data-Security Ideas Emerged in the Equifax Hearing*, BLOOMBERG TECH. (Oct. 3, 2017, 7:40 PM), https://www.bloomberg.com/news/articles/2017-10-03/five-data-security-ideas-brought-up-during-the-equifax-hearing.

163. H.R. 3896; Feinberg, *supra* note 162; Jimmy H. Koo, *What is Informational Injury? The FTC Wants to Know What Folks Think Is Enough Harm to Take Action*, BLOOMBERG PRIVACY & SECURITY BLOG (Nov. 3, 2017), https://www.bna.com/informational-injury-ftc-b73014471670/; Surane, *supra* note 162.

164. H.R. 3896.

165. *Id.*

166. *See* Ryan Moshell, *. . . And Then There Was One: The Outlook for A Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L. REV. 357, 373 (2005) (showing that businesses are in favor of self-regulation as it has allowed them not to realize any deterrent costs over maintaining a lack luster data security system).

167. H.R. 3896.

168. *Id.*

notice to customers of the data breach.[169] Furthermore, businesses would now be required to train and retrain persons who have access to personal information.[170] These new duties are nearly a direct response to many recent data breaches where staff were undertrained or follow insufficient procedures.[171]

In addition to new duties for businesses, if there is a data breach, the Commission would be responsible for enforcing the above duties to facilitate the purpose of the bill and be given the option to audit the covered entities security systems.[172] The Commission would no longer have to rely upon consent decrees for enforcement and thus, would be able to bypass the new substantial hurdle created by the Eleventh Circuit.[173] More importantly, by Congress enacting a bill regarding data security and the Commission's position, the Commission would no longer need to hide behind their interpretation powers of section 5 of the FTC Act to pursue businesses over violations of data security if a data breach has occurred.[174] The core issue in LabMD would be dissolved, as the Commission would directly be given the power to pursue businesses that are found to be in the violation of the new requirements and would not have to ground an unfairness claim in legal standard.[175] Also, it would also have the ability to proactively monitor businesses' data security practices and force updates or changes to better protect consumers data once a data breach has occurred.[176] Moreover, the Commission would no longer be able to or be required to use their dated "dynamic" case-by-case approach to tackle cases.[177]

H.R. 3896 would bring the U.S. one step closer to providing proper consumer protection. It would force and give the Commission the authority to thoroughly audit businesses that had exposed consumer data, as well as

169. *Id.*

170. *Id.*

171. *See* LabMD, Inc. v. FTC, 678 Fed. App'x 816, 818 (11th Cir. 2016) (finding breach was caused by poor training because the billing manager used a work computer to use a peer-to-peer sharing program); Complaint, *supra* note 137; Nelson & Simek, *supra* note 137; Millman, *supra* note 137 (showing website was hacked because of use of outdated systems); Newman, *supra* note 156 (noting failure by staff to patch a new vulnerability of their systems).

172. H.R. 3896.

173. *See supra* Part II; *see also* Frankel, *supra* note 120 (stating the 11th Circuit's "well-established legal standard" is a substantial hurdle for the Commission).

174. *See supra* Part I and Part II.B.

175. *See* LabMD, Inc. v. FTC, 894 F.3d 1221, 1229 (11th Cir. 2018); *LabMD*, 678 Fed. App'x 816; H.R. 3896; *supra* Part I;.

176. *See* H.R. 3896; *supra* Part II.

177. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 254 n.19 (3d Cir. 2015) (finding that the Supreme Court has allowed an agency where a generalized standard framework would be "doubtful," case-by-case analysis is permissible); H.R. 3896; Carson, *supra* note 54.

put an additional duty upon businesses to take increased preventative measures against security breaches.[178] However, even with all the positives, H.R. 3896 would only improve the situation partially, and a more comprehensive governmental data security system would have to be adopted for the Commission to more effectively protect consumer's online data.[179]

B. Strengthening H.R. 3896

H.R. 3896 greatly improves the Commission's position with asserting data security violations, but the bill is wanting in its pre-data breach protections for consumers.[180] The bill only speaks to expanding enforcement actions after a data breach has occurred and not of preemptive measures.[181] The needed substantial improvements over H.R. 3896 would give the Commission an active duty to create national standards and assign businesses an active duty to protect consumer's data.[182] Congress can remedy this issue by mirroring HIPAA and Health and Human Services ("HHS") in their protection of highly sensitive medical data.[183]

1. Improving Regulatory Oversight

With the creation of HIPAA in 1996, HHS began publishing national standards for the protection of health information.[184] The standards are meant to protect the individual's health information while promoting the adoption of new technologies, but also to be "flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's particular size, organizational structure, and risks to consumer's [electronic protected health information]."[185] The general rules give health care providers a duty to not only "maintain

178. *See LabMD*, 678 Fed. App'x 816; H.R. 3896; *supra* Part I.

179. *See* Moshell, *supra* note 166; *see also* Matthew Wilson, *Reducing Legal Risks: Online Commerce, Information Security, and the World*, 33 WYO. LAW. 24 (2010).

180. *See supra* Part III.A.1.

181. H.R. 3896.

182. Brian Fung & Hamza Shaban, *The FTC is Investigating the Equifax Breach. Here's Why That's a Big Deal,* WASH. POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/?utm_term=.ab828abae890; Margaret Rouse, *HIPAA (Health Insurance Portability and Accountability Act),* SEARCH HEALTH IT (July 2017), http://searchhealthit.techtarget.com/definition/HIPAA; Surane, *supra* note 162..

183. Rouse, *supra* note 182.

184. U.S. DEP'T OF HEALTH & HUM. SERVS., *Summary of the HIPAA Security Rule* (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

185. *Id.*

reasonable and appropriate administrative, technical, and physical safeguards," but also an active duty to "[i]dentify and protect against reasonably anticipated threats to the security or integrity of the information."[186] If applied to the business world, there would now be the requirement to, whether or not there was a detected data breach, a fiduciary duty to consumers to actively and reasonably protect consumer's data.[187]

By following the HHS, the Commission could still maintain their more hands-off approach by creating this duty for businesses and regularly establish scalable national standards, yet protect consumer's sensitive data.[188] H.R. 3896 does not go far enough though, as it does not assign an active duty to businesses, nor provide a finely wrought list of objectives for businesses to follow properly, or at least provide bare minimum protection for consumers.[189] If the Commission is given the duty to create and maintain national standards such as the HHS is required to, the Commission will still be able to be as dynamic as they want to be.[190]

2. Increasing Financial Accountability

Lastly, another abysmal part of H.R. 3896 and the status quo is that there is currently low accountability for businesses to comply with standards and for allowing a major data breach to occur.[191] Increased accountability in the monetary sense could use the profit seeking motivations of businesses for the consumer's benefit and for more effective compliance to the standards that would be created by the Commission.[192]

---

186. *Id.* (explaining the four general rules as: ensure the confidentiality, integrity, and availability of all electronically protected health information they create, receive, maintain, or transmit; identify and protect against reasonably anticipated threats to the security or integrity of the information; protect against reasonably anticipated, impermissible uses or disclosures; and ensure compliance by their workforce).

187. *Id.*

188. *See* Rouse, *supra* note 181.

189. *See supra* Part III.A.1.

190. *See* Carson, *supra* note 54; *NAFCU Keep Push for National Data Security Standard As Equifax Hearings Wrap Up*, NAT'L ASS'N OF FEDERALLY-INSURED CREDIT UNIONS (Oct. 6, 2017),https://www.nafcu.org/News/2017_News/October/NAFCU_keeps_push_for_national_data_security_standard_as_Equifax_hearings_wrap_up/;
supra Part II.

191. Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (2017).

192. EUROPEAN PARLIAMENT POL'Y DEP'T CITIZEN'S RIGHTS AND CONST. AFF., *A Comparison Between US and EU Data Protection Legislation for Law Enforcement* (2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf; Danielle D'Onfro, *The Best Way to Hold Equifax Accountable*, WASH. POST (Sept. 14, 2017), https://www.washingtonpost.com/opinions/equifax-doesnt-owe-anyone-anything-but-it-doesnt-have-to-be-this-way/2017/09/14/517c2ef6-98c7-11e7-b569-3360011663b4_story.html?utm_term=.05d657694d5e.

This increased financial accountability could either come in the form of an express private cause of action[193] or by substantially increasing the penalty that the Commission could levy against the infracting business.[194] Businesses often only experience accountability in the form of a few weeks of bad press and potentially a comparatively small fine by the Commission.[195]

For instance, a year after the Equifax's data breach that compromised the sensitive data of over 145 million consumers, the company made more than $3 billion in revenue, the stock price bounced back, and Equifax has not been charged for any data breach violations by the Consumer Financial Protection Bureau and the Federal Trade Commission.[196] Equifax has even escaped any actions or financial penalties from state agencies by merely agreeing with eight states to strengthen their cybersecurity programs to prevent another breach.[197] As of this moment, the message surrounding Equifax is that the only accountability a business may face is in the form of bad press.[198] Applying these fines or creating this cause of action would increase compliance and may actually promote the self-regulation model that the industry so desires.[199]

CONCLUSION

As internet commerce continually expands throughout the U.S., the government in the form of the Commission must take a more active role in protecting consumers sensitive data.[200] Much of the information stolen or leaked through insecure or outdated data security systems is sensitive information that cannot be replaced or changed and can cause grievous financial or emotional harm to consumers for life.[201] Consumers are often

193. *See* Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH L. REV. 783, 810 (2018).

194. D'Onfro, *supra* note 192.

195. *Id.*; Zeynep Tufekci, *Equifax's Maddening Unaccountability,* N.Y. TIMES (Sept. 11, 2017), https://www.nytimes.com/2017/09/11/opinion/equifax-accountability-security.html.

196. Patrick Rucker, *Exclusive: U.S. Consumer Protection Official Puts Equifax Probe On Ice Sources*, REUTERS (Feb. 4, 2018), https://www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ; Whittaker, *supra* note 151.

197. *Id.; see also Governor Cuomo Announces Action to Protect New Yorkers' Private Information Held by Credit Reporting Companies*, N.Y. STATE DEP'T. FIN. SERV. (June 25, 2018), https://www.dfs.ny.gov/about/press/pr1806251.htm.

198. Whittaker, *supra* note 151.

199. *See* D'Onfro, *supra* note 192; Surane, *supra* note 162; *supra* Part I.B.

200. *See supra* Part II and Part III.

201. *See supra* Part II.B.1.

unable to bring suits themselves with the Commission and now face substantial hurdles over their ability to as well.[202]

One of the solutions presented, H.R. 3896, would provide some benefit to consumers, although a more expansive model passed by Congress, similar in the form of HIPAA would provide adequate protection for consumers.[203] Under a HIPAA style expansion of regulatory oversight, the Commission would be able to provide scalable national standards and the ability to enforce violations if need be.[204] Additionally, if passed in conjunction with increased accountability measures, businesses would be compelled to comply and provide proper protection of consumer's sensitive data for the sake of remaining profitable.[205] The massive data breach of the key institution, Equifax, must be the wake-up call for the Commission and Congress to take a more active role in keeping Americans' sensitive data secure.

*Giordan Roque**

202. *See* Koo, *supra* note 163; *supra* Part II.

203. *See supra* Part III.A.2.

204. *See supra* Part III.

205. *See supra* Part III.

* J.D., Southwestern Law School, 2019; B.A., Political Science, University of Southern California, 2015. I would like to thank Professor Kelly Strader, Taylor Condit, Andie Johnson, Jasen Talise, Rosio Flores, William Dietz, Gevork Gazaryan, Madelynn Hefner, Yamili Gonzalez, Brandon Faus, David Zakharian, and Suren Agadzhanov for their help in developing and editing this paper. I would also like to thank my family, especially my mother, as well as my dogs for their help and support.