Catholic University Law Review

Volume 66
Issue 4 *Summer2017*

Article 9

11-2-2017

Who Are the Real Cyberbullies: Hackers or the FTC? The Fairness of the FTC's Authority in the Data Security Context

Jaclyn K. Haughom

Who Are the Real Cyberbullies: Hackers or the FTC? The Fairness of the FTC's Authority in the Data Security Context

Cover Page Footnote
Juris Doctor 2017, The Catholic University of America, Columbus School of Law. I would like to thank my family and friends for their continuous support, especially my father James Haughom for assisting me in formulating the legal issues on which this Comment is based. I would also like to thank Professor Christopher W. Savage, Partner at Davis Wright Tremaine LLP, for the invaluable guidance and expertise he provided throughout the progression of this Comment.

WHO ARE THE REAL CYBERBULLIES: HACKERS OR THE FTC? THE FAIRNESS OF THE FTC'S AUTHORITY IN THE DATA SECURITY CONTEXT

Jaclyn K. Haughom[+]

From 2013 to 2014, mass data breaches compromised the payment card information of 248 million Americans.[1] Society's ever-increasing use of technology in its everyday practices, from paying bills to corresponding with co-workers, intensifies the threat of mass data breaches.[2] A data breach occurs when personally identifiable information (PII) is lost, stolen, or accessed without authorization, resulting in a potential compromise of confidential data.[3]

Data breaches expose consumer information—such as Social Security numbers, personal account passwords, and financial or medical information—to outside parties, often resulting in identity theft.[4] Certain high-profile mass data breaches have gained substantial media attention,[5] with large corporations such

---

[+] Juris Doctor 2017, The Catholic University of America, Columbus School of Law. I would like to thank my family and friends for their continuous support, especially my father James Haughom for assisting me in formulating the legal issues on which this Comment is based. I would also like to thank Professor Christopher W. Savage, Partner at Davis Wright Tremaine LLP, for the invaluable guidance and expertise he provided throughout the progression of this Comment.

1. N. ERIC WEISS & RENA S. MILLER, CONG. RES. SERV., R43496, THE TARGET AND OTHER FINANCIAL DATA BREACHES: FREQUENTLY ASKED QUESTIONS 1 (2015). The Target breach of 2013 affected 40 million payment cards, the Adobe breach of 2013 affected 152 million payment cards, and the Home Depot breach of 2014 affected 56 million payment cards. *Id.*

2. *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Prepared Statement of the Federal Trade Commission (Mar. 26, 2014), *in Protecting Personal Consumer Information from Cyber Attacks and Data Breaches: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 113th Cong. 16–21 (2014) ("[H]ackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses.").

3. GINA STEVENS, CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 1 (2014). A data breach is defined as "a loss or theft of, or other unauthorized access to, sensitive personally identifiable information (PII) that could result in the potential compromise of the confidentiality or integrity of data." *Id.*; *see also* Allison Grande, *FTC Steps Up Privacy Enforcement, with No Slowdown in Sight*, LAW360 (July 23, 2014, 7:36 PM), http://www.law360.com/articles/559907/ftc-steps-up-privacy-enforcement-with-no-slowdown-in-sight (reporting on the FTC's enforcement actions against companies "over allegedly misleading privacy promises and lax data security").

4. Ramirez, *supra* note 2, at 16–17. "These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information." *Id.* at 16.

5. The U.S. Office of Personnel Management (OPM) was a victim to a mass data breach in June 2015, when the sensitive information of 21.5 million current, former, and prospective Federal

as Target, Home Depot, JPMorgan Chase, Sony, and Adobe falling victim to recent breaches.[6] In the Target data breach, the personal information of millions of customers was compromised.[7] Following the breach, Gregg Steinhafel, CEO, president, and Chairman of the Target board of directors, resigned,[8] when affected consumers filed a class action suit against the corporation.[9]

Responding to the increasing frequency of major data breaches, Edith Ramirez, Chairwoman of the Federal Trade Commission (FTC) has asserted that Congress should meet the "longstanding, bipartisan call" for enhanced federal data security legislation.[10] Lawmakers and government agencies alike are calling for legislation that not only punishes cybercriminals for data breaches, but also imposes liability on entities for failing to properly protect against cyber-attacks.[11]

The FTC is the U.S. government's primary consumer protection agency and the country's lead enforcer against companies subject to data breaches.[12] The FTC began its involvement with consumer privacy protection in 1995.[13] With the increase of data breaches, the FTC has increased the number and scope of its investigations into data security practices.[14] No statute explicitly grants the FTC

---

government employees was jeopardized. *Cybersecurity Resource Center: Cybersecurity Incidents*, U.S. OFF. OF PERS. MGMT., https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited Feb. 12, 2017). Following the OPM breach, Katherine Archuleta, Director of OPM, resigned. Bill Chappell, *OPM Director Archuleta Resigns in Wake of Data Breaches*, NPR (July 10, 2015, 12:43 PM), http://www.npr.org/sections/thetwo-way/2015/07/10/421783403/opm-director-archuleta-resigns-in-wake-of-data-breaches. This breach is outside the scope of this Comment because it involved a public government entity, rather than a private company.

6. WEISS & MILLER, *supra* note 1, at 1. The Heartland Breach of 2009 and the TJX breach of 2007 are examples of other financial breaches. Other breaches of confidential, nonfinancial data include: The Sony Corporation (PlayStation Network) in 2011; Sony Picture Entertainment in 2014; and TriCare Management Activity in 2011. *Id.*

7. It should be noted that mass data breaches have also occurred internationally. In 2014, South Korea experienced "the theft of 220 million records containing personal information and passwords," and in 2012, Shanghai Roadway & Marketing in China had 150 million records stolen. *Id.*

8. Press Release, Target Corp., Statement from Target's Board of Directors (May 5, 2014), http://pressroom.target.com/news/statement-from-targets-board-of-directors.

9. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

10. Ramirez, *supra* note 2, at 17 ("Never has the need for [data security and breach notification] legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress must act.").

11. *See generally* STEVENS, *supra* note 3.

12. *Id.* at 1 ("The protection of consumers from anticompetitive, deceptive, or unfair business practices is at the core of the FTC's mission. As part of that mission, the FTC has been at the forefront of the federal government's efforts to protect sensitive consumer information from data breaches, and to regulate cybersecurity." (footnote omitted)).

13. *Id.* at 3. Initially, the FTC encouraged self-regulation in the industry for protecting consumer privacy. "After assessing its effectiveness, however, the FTC reported to Congress that self-regulation was not working." *Id.*

14. *Id.* at 1.

the authority to combat data breaches, but the FTC has done so through a broad interpretation of Section 5 of its enabling statute, the Federal Trade Commission Act (FTCA).[15]

Since 2002, the FTC has relied on Section 5 to settle fifty data breach cases with private companies for "failure to adequately safeguard customers' sensitive personal information."[16] In these settlements, the FTC issues a consent decree in which the affected company agrees to take measures to deter problematic data security practices, often without admitting that it violated the law.[17] However, as the FTC continues to take action against businesses whose unfair data security practices have led to data breaches, private companies are questioning the agency's authority to do so.[18] As a result of challenges to its authority, the FTC is pushing for federal legislation to "strengthen its existing authority governing data security standards on companies."[19] The passage of federal data security legislation, such as the Data Breach Notification and Punishing Cyber Criminals Act of 2015,[20] would grant the FTC explicit authority to enforce against data breaches.

> As the number of data breaches continues to soar, so too do the number of FTC investigations into lax data security.
>
> Data breaches have become almost ubiquitous in every sector of the economy. Businesses, financial and insurance services, retailers and merchants, educational institutions, government and military agencies, healthcare entities, and non-profit organizations have suffered cyber intrusions into their computer networks.

Id. (footnotes omitted).

15. 15 U.S.C. § 45 (a)(1) (2012); STEVENS, *supra* note 3, at 4.

16. STEVENS, *supra* note 3, at 6.

17. *See, e.g.*, Dave & Buster's, Inc., 149 F.T.C. 1449 (2010) (consent order); *see also* DSW, Inc., 141 F.T.C. 2 (2006) (consent order). In its investigations, the FTC found that many of the businesses engaged in unfair data security practices, which resulted in the subsequent data breaches that harmed consumers. Upon such a finding, the business that is the subject of the investigation may elect to either enter a settlement agreement with the FTC or dispute the charges. STEVENS, *supra* note 3, at 6. A settlement agreement with the FTC typically requires the business to implement adequate data security measures to prevent further breaches. The consent order is then placed on record for public comment. *Id.* However, if the business "contests the charges, an Administrative Law Judge (ALJ) issues an 'initial decision' recommending either entry of an order to cease and desist or dismissal of the complaint." *Id.* Then, either party may appeal the decision to the full FTC. Additionally, the business may file for review of the full FTC decision to any appellate court, and, if the court affirms the FTC's order, it enters an order of enforcement. *Id.* "The losing party may [then] seek Supreme Court review." *Id.*

18. *See, e.g.*, LabMD, Inc., 2014-1 Trade Cas. (CCH) P78,784, 2014 FTC LEXIS 2 (F.T.C. Jan. 16, 2014); *see also* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244–46 (3d Cir. 2015) (rejecting a hotel company's argument that deficient cybersecurity falls outside of the FTC's scope to prohibit unfair practices).

19. Ramirez, *supra* note 2, at 20. The FTC also supports federal legislation that would "require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach." *Id.*

20. Data Breach Notification and Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. (2015). Senator Mark Steven Kirk (R-Ill.) introduced the Act to the Senate Committee on Commerce, Science, and Transportation on April 21, 2015. *Id.*

Part I of this Comment examines the FTC's exercise of authority with regard to data breaches under Section 5 of the FTCA, noting that, over the course of many actions, the FTC's authority on such matters was not contested, resulting in settlements between the parties. Part II discusses how certain companies have challenged the FTC's authority to take enforcement actions against data breaches, and how recent court rulings may affect the results of a potential Target breach investigation. Part III discusses how recently introduced federal legislation may deter data breaches by clearly establishing the FTC's authority while also proposing an extension of this legislation to ensure that liability is imposed against all entities that are subject to data breaches.

I. THE FTC'S AUTHORITY TO ENFORCE AGAINST DATA BREACHES

A. Applying Section 5 to Data Security Practices

The FTC has grounded its authority to take enforcement action against companies subject to data breaches primarily in Section 5 of the FTCA.[21] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[22] Under a broad interpretation of Section 5, the FTC has considered the failure to protect private consumer information to be an "unfair or deceptive act."[23] On this theory, a private company violates Section 5 when its improper data security practices make it likely for a third party to invade the company's computer systems.[24]

The FTC uses a reasonableness standard when looking at the adequacy of a company's data security system,[25] exemplified by the current statutes and rules enforced to protect consumer data.[26] When evaluating a company's data

21. Ramirez, *supra* note 2, at 17 ("[T]he [FTC] enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act." (citing 15 U.S.C. § 45(a) (2012))).

22. 15 U.S.C. § 45(a)(1)–(2).

23. STEVENS, *supra* note 3, at 3. As an example of the FTC's authority in the data security context, in March 2012, the FTC released a privacy report, which set forth "best practices" for companies that accumulate data "that can be reasonably linked to a consumer, computer, or device. Entities that collect only non-sensitive data from fewer than 5,000 consumers per year and that do not share the data with third parties would not have to adhere to the practices." *Id.* at 4.

24. Ramirez, *supra* note 2, at 17 ("A company's failure to reasonably safeguard consumer data [is] an unfair practice.").

25. FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (Jan. 31, 2014), http://ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [hereinafter 50TH SETTLEMENT STATEMENT] ("The touchstone of the [FTC]'s approach to data security is reasonableness . . . . [T]he [FTC] has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.")

26. Ramirez, *supra* note 2, at 17. The Gramm-Leach-Bliley Act (GLB Act), 15 U.S.C. § 6801(b) (2012), sets "data security requirements for non-bank financial institutions." *Id.* The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681e, 1681w (2012), requires consumer reporting agencies to protect against impermissible disclosure of sensitive consumer information. The

security practices, the "measures [taken] must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[27] The tenets of a reasonable data security program under this standard are that a company should:

> [1] know what consumer information they have and what employees or third parties have access to it[;] . . . [2] limit the information they collect and retain based on their legitimate business needs[;] . . . [3] protect the information they maintain by assessing risks and implementing protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers[;] . . . [4] properly dispose of information that they no longer need[;] . . . [5] have a plan in place to respond to security incidents, should they occur.[28]

Although "unfair" and "deceptive" acts are covered in the same statutory section, they are different concepts. Acts of deception occur "only when business conduct causes tangible harm to consumers who acted reasonably and were misled."[29] Unfairness, however, "incorporat[es] not only the harms to aggrieved consumers but also any benefits to consumers or to competition more generally."[30]

To determine whether a company's failure to protect against a data breach has violated Section 5 of the FTCA, the FTC looks to whether the conduct meets the requirements of the unfairness test.[31] Under that test, an individual or entity has taken an unfair act in or affecting commerce if the conduct "[1] causes or is likely to cause substantial injury to consumers[, 2] which is not reasonably

---

Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2012), protects against collection of children's information online. "Reasonableness is the foundation of the data security provisions of each of these laws." *Id.*

27. 50TH SETTLEMENT STATEMENT, *supra* note 25, at 1.

28. *Id.*

29. Alden F. Abbott, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, LEGAL MEMORANDUM (Heritage Found., Washington, D.C.), Sept. 10, 2014, at 3, http://thf_media.s3.amazonaws.com/2014/pdf/LM137.pdf ("The FTC defines 'deception' as involving a 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.'").

30. *Id.* at 4 (quoting Joshua D. Wright, Commissioner, Fed. Trade Comm'n, The Economics of Digital Consumer Protection: One Commissioner's View, Remarks to TechFreedom and the International Center for Law and Economics (July 31, 2014), https://www.ftc.gov/system/files/documents/public_statements/573061/010731techfreedom.pdf). The unfairness prong "necessarily calls for cost-benefit analysis, since it weighs potential efficiencies against consumer harm, which makes it a more stringent test than deception." *Id.* at 3–4 (footnote omitted).

31. STEVENS, *supra* note 3, at 4, 6–7 ("According to recent testimony by FTC Chairwoman Edith Ramirez, using the deceptive prong of its statute, the FTC has settled more than [thirty] matters challenging companies' express and implied claims about the security they provide for consumers' personal data . . . .").

avoidable by consumers themselves[,] and [3] not outweighed by countervailing benefits to consumers or to competition."[32]

B. The FTC's Rulemaking Authority

Although the FTCA does not enumerate specific unfair acts that the FTC's broad Section 5 authority applies, it does empower the FTC to remedy unfair practices in specific industries through rulemaking.[33] The FTC has rulemaking authority under statutes such as: the Do-Not-Call Implementation Act of 2003,[34] the Children's Online Privacy Protection Act (COPPA),[35] the Fair and Accurate Credit Transactions Act of 2003,[36] and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.[37] Under COPPA, the FTC can directly regulate data security practices that involve obtaining personal information from children.[38] By establishing rules that website operators must follow to protect children from crimes such as identity theft,[39] the FTC bans specific acts that constitute "unfair or deceptive acts or practices in or affecting commerce" within the meaning of Section 5.[40] However, the COPPA rulemaking statute only allows the FTC to promulgate rules regarding data security practices in the specific context of children's use of the Internet.[41] Therefore, unless the FTC obtains rulemaking authority for data security generally,[42] it will not be able to set applicable requirements governing the data security measures taken by private companies.[43]

---

32. 15 U.S.C. § 45(n) (2012); *see also*, Ramirez, *supra* note 2, at 17.

33. STEVENS, *supra* note 3, at 4. *See* 15 U.S.C. § 57a (a)(2) (2012) ("The [FTC] shall have no authority under this Act, other than its authority under this section, to prescribe any rule with respect to unfair or deceptive acts or practices in or affecting commerce . . . ."); *see also A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [hereinafter *Brief Overview of the FTC's Authority*]. The FTC is also able to seek civil penalties for violations of administrative orders. Ramirez, *supra* note 2, at 20 n.35 (citing 15 U.S.C. § 45(l)).

34. 15 U.S.C. §§ 6151–6152 (2012).

35. 15 U.S.C. § 6502(b) (2012).

36. 15 U.S.C. § 1681m(e) (2012).

37. 15 U.S.C. §§ 7701–7713 (2012).

38. 15 U.S.C. § 6502(b)(1).

39. Ramirez, *supra* note 2, at 2.

40. *Brief Overview of the FTC's Authority*, *supra* note 33 (quoting 15 U.S.C. § 45(a)(1)).

41. 15 U.S.C. § 6502(b).

42. *See* Ramirez, *supra* note 2, at 14–15.

43. For comparison, the European Union adopted generally applicable data privacy laws, which recognize an individual's right to protect his or her personal data.

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

C. The Data Breach Notification and Punishing Cyber Criminals Act of 2015

In April 2015, Senator Mark Steven Kirk (Republican, Illinois) introduced the Data Breach Notification and Punishing Cyber Criminals Act of 2015 to the Committee on Commerce, Science, and Transportation.[44] This Act serves "to require notification of information security breaches and to enhance penalties for cyber criminals, and for other purposes."[45] Generally, the Act requires an entity to notify a citizen or resident of the United States when it falls victim to a data breach in which the individual's PII has been accessed, or is at risk of being accessed, without authorization.[46] A significant aspect of Senator Kirk's proposed bill is that it explicitly sets forth the FTC's authority to take enforcement action against data breaches in this context.[47] Although it is still in the legislative process, if the bill goes into effect it will provide the FTC with its desired authority in general data security matters, thereby preventing future suits that question the FTC's power in this realm.

D. Settlements: The Early Data Security Cases

The FTC has brought and settled fifty data security cases since 2002.[48] In these cases, the FTC first conducted an investigation of the company's data security practices.[49] If the FTC did not find the company's data security practices to be reasonable, it then filed an administrative action against the company for failure to take the appropriate measures to protect against data breaches,[50] with the company typically agreeing to a consent decree.[51] The consent decree typically required the company to implement certain data security measures and obtain audits by third party data security experts for a period of time determined by the FTC.[52] The FTC's successful settlements with

---

Charter of Fundamental Rights of the European Union, art.8, 2012 O.J. (C 326) 2, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

44. Data Breach Notification and Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. (2015).

45. *Id.*

46. *Id.* § 3(a)(1).

47. *Id.* § 4(c)(1)–(2).

48. STEVENS, *supra* note 3, at 6.

49. Ramirez, *supra* note 2, at 17.

50. *Id.* (discussing how the FTC charges businesses with "failing to provide reasonable protections for consumer's personal information").

51. The agreed-to consent decree terminates the FTC's investigation. *See* Abbott, *supra* note 29, at 4 ("[T]he FTC has filed and settled over [fifty] cases against private companies, arguing that they compromised consumers' security by using deceptive or ineffective (unfair) practices in storing their data. . . . These cases involved complaints that would have been adjudicated administratively within the commission had they not been settled.").

52. STEVENS, *supra* note 3, at 7 ("These measures are typical of the measures required of companies in the FTC's consent agreements to remedy failures to provide reasonable security protections."); *see also* Ramirez, *supra* note 2, at 18 (providing examples of settlement agreements in which companies were required to obtain independent audits).

businesses have prevented further harmful data security practices, required companies to implement stronger preventive measures to protect consumer information, raised awareness of data security risks, and emphasized the need for appropriate security measures.[53]

Take, for example, *United States v. ChoicePoint, Inc.*,[54] which was the first data security enforcement action taken by the FTC. In that case, ChoicePoint, Inc., a publicly traded consumer data broker, experienced a data breach in 2004 that compromised information relating to over 163,000 consumers.[55] The FTC alleged that ChoicePoint failed to implement "reasonable procedures to screen prospective subscribers and turned over consumers' sensitive personal information to subscribers whose applications raised obvious 'red flags,'"[56] in violation of Section 5 of FCTA.[57] In its settlement with the FTC, ChoicePoint agreed to pay $10 million in civil penalties, $5 million toward consumer redress, and implement and maintain a data security program "reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[58]

Another early enforcement action by the FTC involved Dave & Buster's, Inc.[59] There, the entertainment corporation fell victim to a data breach, which exposed the credit and debit card information of approximately 130,000 consumers to hackers, resulting in "several hundred thousand dollars in

---

53. Ramirez, *supra* note 2, at 17–18.

> The [FTC]'s [fifty] settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.

Id. at 17.

54. No. 1:06-CV-0198, 2006 U.S. Dist. LEXIS 98749, at *1 (N.D. Ga. Feb. 15, 2006).

55. STEVENS, *supra* note 3, at 7 ("In 2006, The FTC brought its first data security enforcement action against the data broker ChoicePoint after ChoicePoint disclosed a data breach involving the personal information of 163,000 persons." (footnote omitted)). Although, the enforcement action was filed in 2006, the breach was discovered in October 2004. Notably, ChoicePoint waited over three months to notify the approximately 30,000 California consumers whose data was compromised, as mandated by a 2003 California law. *See FAQ on ChoicePoint*, AM. CIV. LIBER. UNION https://www.aclu.org /other/faq-choicepoint?redirect=faq-choicepoint (last visited Feb. 16, 2017) ("Only after letters to California consumers became public did the company . . . notify consumers living in other states.").

56. Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (Jan. 26, 2006), https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

57. The FTC brought suit against ChoicePoint for violating Section 5 of FCTA by engaging in "unfair or deceptive acts or practices," through its failure to protect personal information collected from or about consumers. *ChoicePoint, Inc.*, 2006 U.S. Dist. LEXIS 98749, at *1.

58. *Id.* at *32–33.

59. Dave & Buster's, Inc., 149 F.T.C. 1449 (2010) (consent order).

fraudulent charges."[60] Dave & Buster's was subsequently charged with failing "to take reasonable steps to secure this sensitive personal information on its computer network," in violation of Section 5.[61] As part of its settlement with the FTC, Dave & Buster's agreed to initiate a data security program to adequately protect its consumers' sensitive personal information.[62]

The FTC's action against DSW, Inc.[63] involved a much larger breach. There, hackers stole more than 1,400,000 credit and debit card numbers, more than 96,000 checking account numbers, and driver's license numbers of the footwear company's customers.[64] With the vast number of accounts compromised, some with fraudulent charges, many customers were forced to close their checking accounts.[65] According to the FTC, DSW violated Section 5 because it failed, "to employ reasonable and appropriate security measures to protect personal information and files[, which] caused or [were] likely to cause substantial injury."[66] As in many other data security cases that resulted in settlement agreements, the FTC required DSW to "establish and implement, and thereafter maintain" a data security program that would protect the confidential information of its consumers.[67]

In the FTC's fiftieth data security settlement action,[68] the FTC alleged that GMR Transcription Services, Inc. (GMR) "engaged in deceptive and unfair information security practices that exposed the personal information of thousands of consumers online."[69] GMR transcribes audio files for various entities, including hospitals, healthcare providers, and universities.[70] At the time of this action, GMR predominantly outsourced the actual task of transcribing the audio files to independent service providers.[71] GMR assigned Fedtrans Transcription Services, Inc. (Fedtrans) to transcribe all of GMR's medical audio

60. *Id.* at 1452.

61. Press Release, Fed. Trade Comm'n, Dave & Buster's Settles FTC Charges It Failed to Protect Consumers' Information (Mar. 25, 2010), https://www.ftc.gov/news-events/press-releases/2010/03/dave-busters-settles-ftc-charges-it-failed-protect-consumers.

62. *Dave & Buster's, Inc.*, 149 F.T.C. at 1462.

63. DSW, Inc., 141 F.T.C. 117 (2006).

64. *Id.* at 120.

65. *Id.*

66. *Id.*

67. *Id.* at 123.

68. GMR Transcription Servs., Inc., 2015-1 Trade Cas. P17,070, 2014 WL 4252393 (F.T.C. Aug. 14, 2014); Press Release, Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Jan. 31, 2014), http://www.ftc.gov/news-events/press-releases-2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

69. Press Release, Fed. Trade Comm'n, FTC Approves Final Order in Case Against GMR Transcription Services (Aug. 21, 2014), https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-order-case-against-gmr-transcription-services.

70. *GMR Transcription Servs., Inc.*, 2014 WL 4252393, at *1.

71. *Id.*

files, which included personal information such as names, dates of birth, and medical histories.[72] Despite GMR's claims that its security systems were "highly secure" and compliant with federal regulations, GMR failed to discover that Fedtrans was storing its files in a file transfer application that made the files available in "clear readable text . . . without authentication."[73] As a result, a major search engine discovered the Fedtrans files, rendering them readily accessible to anyone using the search engine.[74]

In 2014, the FTC determined that GMR's omissions constituted an unfair or deceptive act in violation of Section 5 because GMR "could have corrected [its] security failures using readily available, low-cost security measures" and failed to do so.[75] Under the settlement, GMR is prohibited from misrepresenting how it maintains and secures private consumer information and is required to initiate and maintain adequate data security measures.[76] As entities, such as GMR and DSW, readily agreed to the terms of the FTC's consent decrees, the FTC's authority to take enforcement action against data breaches under Section 5 remained largely unchallenged for quite some time.

E. Challenging the FTC's Section 5 Authority

Given that the FTC has successfully settled data security actions against fifty companies, there have not been many notable judicial decisions regarding these issues.[77] However, two private companies separately challenged the FTC's authority to take action in data breach cases, arguing that Section 5 does not grant the FTC the power "to directly regulate" unfair data security practices.[78] At least in one case, the courts sided with the agency and determined that the FTC, under a broad interpretation of Section 5, could take enforcement action against companies that do not take adequate steps to prevent data breaches.[79] In upholding the FTC's authority, the courts acknowledged that the FTCA does not define acts or practices that are unfair because Congress "designed the term [unfair practices] as a 'flexible concept with evolving content,'"[80] as legislators

72. *Id.* at *1–2.

73. *Id.* at *2–3.

74. *Id.*

75. *Id.* at *4.

76. *Id.* at *6.

77. *See* STEVENS, *supra* note 3, at 6–7 ("Because most of the FTC's privacy and data security cases, and almost all of its COPAA and GLBA cases, were resolved with settlements or abandoned, there are few judicial decisions addressing the FTC's authority to regulate the data security practices of companies which have suffered a data breach.").

78. LabMD, Inc., 2014-1 Trade Cas. (CCH) P78,784, 2014 FTC LEXIS 2 (F.T.C. Jan. 16, 2014); FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244–46 (3d Cir. 2015).

79. *Wyndham Worldwide Corp.*, 799 F.3d at 248–49 (disagreeing with Wyndham's assertion that the FTC lacked statutory authority over cybersecurity issues).

80. *Id.* at 243. The FTC has also reiterated congressional intent to broadly define unfairness. *See LabMD, Inc.*, 2014 F.T.C. LEXIS 2, at *12–13 (noting that Congress intended for the FTC to determine what is unfair on a case-by-case basis, and that courts have been applying the

of the Act found it "impossible to frame definitions which embrace all unfair practices."[81]

1. Wyndham Worldwide Corp.: No "Unfairness" Authority with Data Security

In *FTC v. Wyndham Worldwide Corp.*,[82] the hotel and resort chain fell victim to three cybersecurity breaches between 2008 and 2009 in which hackers accessed more than 619,000 payment accounts, resulting in at least $10.6 million in fraudulent charges.[83] The FTC brought suit against Wyndham for its "deficient cybersecurity" practices that, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[84] The unfair cybersecurity practices that constituted a Section 5 violation included: storing payment card information "in clear readable text," allowing "the use of easily guessed passwords" to access Wyndham's computer systems, failing to use security measures such as firewalls, and failing to "prevent unauthorized access" to the computer system.[85]

Rather than settling with the FTC, Wyndham contested the allegations.[86] Specifically, Wyndham challenged the FTC's authority under Section 5, claiming that Section 5 did not grant the FTC the authority to pursue a data security breach as an unfair act or practice.[87] In its argument, Wyndham analogized the FTC's overreach of authority to that of the Food and Drug Administration (FDA) in *FDA v. Brown & Williamson Tobacco Corp.*[88] In that case, the U.S. Supreme Court held that, without specific authority over tobacco products, the FDA could not use its general statutory authority to regulate tobacco products.[89] The Court reached this conclusion because Congress had passed subsequent legislation specifically targeted to regulate tobacco products.[90]

"unfairness" factors even though the Act does not expressly provide the FTC's regulating authority over data security matters)

81. H.R. Rep. No. 63-1142, at 19 (1914) (Conf. Rep.) ("There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task.").

82. 799 F.3d 236 (3d Cir. 2015).

83. *Id.* at 241–42.

84. *Id.* at 240 (quoting the complaint filed against Wyndham Worldwide Corporation by the FTC).

85. *Id.* at 240–41.

86. *Id.* at 242.

87. *Id.* at 244 (arguing that the three requirements to determine unfairness are insufficient and that the meaning of "unfair" involves additional requirements).

88. 529 U.S. 120 (2000).

89. *Id.* at 160–61.

90. *Id.* at 160 ("To find that the FDA has the authority to regulate tobacco products, one must not only adopt an extremely strained understanding of 'safety' as it is used throughout the Act—a

Wyndham argued that, similar to *Brown & Williamson*, Congress did not intend to give the FTC the specific authority to regulate data security through its general authority to regulate "unfair acts or practices."[91] As proof of Congress' intention to exclude cybersecurity from the FTC's general authority under Section 5, Wyndham pointed to three subsequent legislative acts that explicitly granted specific authority in the cybersecurity field: the FCRA, the Gramm-Leach-Bailey Act, and the COPPA.[92] "These tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the FTC already had general substantive authority over this field."[93]

In response, the FTC distinguished its conduct from the FDA's in *Brown & Williamson* by explaining that, unlike the statute at issue there, the FTCA gives the agency general authority to take enforcement action against unfair acts or practices, and specific statutes such as FCRA and COPPA are not inconsistent with this notion.[94] The FTC then asserted that proving a substantial harm to consumers from data security actions, such as Wyndham's cybersecurity hacks that exposed "unsuspecting customers to substantial financial injury," was consistent with the FTC's broad authority under Section 5.[95] Agreeing with the FTC, the Third Circuit upheld the FTC's authority to take action against companies experiencing data security breaches under Section 5.[96]

2. LabMD: Section 5 Does Not Apply to Data Breaches

In re LabMD was the first adjudicatory proceeding that challenged the FTC's authority "to regulate or bring enforcement action with respect to the data security practices alleged" under the FTCA.[97] LabMD, Inc., is a cancer-detection testing laboratory based in Atlanta, Georgia. When the FTC received notice that LabMD's files containing private patient information were readily available on a file-sharing network, it began investigating the laboratory's data security practices.[98]

Following its investigation, the FTC filed an administrative complaint against LabMD for "fail[ing] to provide reasonable and appropriate security for" the personal data of 10,000 consumers, which caused harm to consumers and

concept central to the FDCA's regulatory scheme—but also ignore the plain implication of Congress' subsequent tobacco-specific legislation.")

91. *Wyndham Worldwide Corp.*, 799 F. 3d at 247.

92. *Id.*

93. Appellant's Opening Brief at 25, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514).

94. *Wyndham Worldwide Corp.*, 799 F. 3d at 247–49.

95. *Id.* at 245.

96. *Id.* at 259.

97. LabMD, Inc., 2014 FTC LEXIS 2, at *7 (F.T.C. Jan. 16, 2014).

98. *Id.* at *4.

constituted an unfair act or practice in violation of the FTCA.[99] In response, LabMD moved to dismiss the complaint on grounds that the FTC lacked statutory authority to take action against companies subject to data breaches and that "Section 5 does not authorize the FTC to address any data security practices."[100] However, this was a slightly different claim than that raised in *Wyndham Worldwide Corp.*

In *Wyndham Worldwide Corp.*, the contention was that the FTC's authority to deal with "unfair" practices was too ambiguous to be applied to the specific context of data security breaches.[101] LabMD, by contrast, argued that Section 5 of the FTCA did not apply to this type of situation at all.[102] The FTC denied the motion to dismiss, asserting that Congress purposely delegated broad authority to the agency to determine what exactly constitutes an unfair act or practice.[103] LabMD immediately appealed the administrative decision to the federal district court. However, the district court dismissed the case for want of subject matter jurisdiction because the administrative procedure had not reached a final decision by the FTC.[104] On appeal, the Eleventh Circuit affirmed the lower court, holding LabMD's decision to seek review in the federal courts as premature.[105]

3. The Target Breach: Will It Be Subject to FTC Enforcement?

The Target data breach is one of the largest breaches in U.S. history.[106] In November 2013, cybercriminals obtained consumer payment card information from Target's computer systems.[107] Target's security systems detected the breach, but the company failed to take any action.[108] The following month, the Department of Justice notified Target of fraudulent activity on payment cards used in its stores.[109] Then, Target launched a forensic investigation and made a public announcement of the breach.[110] In the course of the investigation, forensic experts discovered that not just credit card numbers, but also encrypted

99. *Id.*; *see* Press Release, Fed. Trade Comm'n, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

100. *LabMD, Inc.*, 2014 F.T.C. LEXIS 2, at *8.

101. *Wyndham Worldwide Corp.*, 799 F.3d at 252, 256 n.21.

102. *LabMD, Inc.*, 2014 F.T.C. LEXIS 2, at *8.

103. *Id.* at *9–10.

104. LabMD, Inc. v. FTC, No. 1:14-cv-00810, 2014 WL 1908716, at *6 (N.D. Ga. May 12, 2014) ("In the absence of final agency action, LabMD's alleged constitutional injuries are not ripe for review.").

105. LabMD, Inc. v. FTC, 776 F.3d 1275, 1280 (11th Cir. 2015).

106. WEISS & MILLER, *supra* note 1 ("The [Target] breach was among the largest in U.S. history.").

107. *Id.* at 2.

108. *Id.*

109. *Id.* at 3.

110. *Id.*

personal identification numbers (PIN) and PII, had been compromised, requiring Target to make subsequent public announcements specifying the information that had been stolen. It announced that the compromised information included 40 million credit and debit card account numbers and the PII of 70 million customers.[111]

Allegedly, the cybercriminals gained access to the credentials of one of Target's vendors and used those credentials to enter Target's vendor billing and invoicing system.[112] From there, the cybercriminals gained access to Target's point-of-sale system (the devices used by consumers to swipe their credit or debit cards) and infected that system with malware.[113] Target's security system received warnings about the malware, but Target initially ignored those warnings, which allowed the malware to spread.[114] The malware then sent the payment card information to other servers. Target, however, also ignored warnings about those data transmissions.[115] Although Target has been in correspondence with the FTC, the details and formalities of the FTC's investigation have not yet been released. In addition to a potential FTC investigation, Target has also been subject to class action lawsuits from customers and banks.[116]

II. HOW THE FTC HAS APPLIED THE UNFAIRNESS TEST TO DATA SECURITY

Despite the FTC's success in bringing forth and settling fifty data security actions, as *Wyndham Worldwide Corp.* and *LabMD, Inc.* illustrate, the FTCA's text does not expressly grant the FTC specific authority to take enforcement action in cybersecurity situations.[117] As Wyndham and LabMD both argued, the FTC lacks clear statutory authority over data security and, furthermore, Congress' enactment of specific data security legislation, such as COPPA, "implicitly repealed the FTC's preexisting authority to enforce Section 5 of the FTC Act in the field of data security."[118] However, courts have determined that

111. *Id.*

112. *Id.* ("Fazio Mechanical Services, which provided heating, ventilation, and air-conditioning (HVAC) services for Target, has said it was used to breach Target's payment system. A Fazio computer authorized to submit contract billing and project information to Target reportedly was compromised by intruders.").

113. *Id.* ("Fazio was the victim of a phishing email containing malware that was used to install other malware in Target's network, including its POS system that records payment card transactions.").

114. *Id.* at 4.

115. *Id.*

116. *Id.* at 6 (stating that over 100 legal actions have been filed against Target following the breach). *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482 (D. Minn. 2015); *see also In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1156–57 (D. Minn. 2014); *see generally* TARGET BREACH SETTLEMENT, https://targetbreachsettlement.com/mainpage/Home.aspx (last updated Feb. 9, 2017).

117. *See* 15 U.S.C. § 45(a) (2012).

118. STEVENS, *supra* note 3, at 8–10.

Congress chose not to name the types of acts that would constitute unfairness,[119] and delegated to the FTC the power to make such determinations on a case-by-case basis.[120]

To determine whether an act or practice is unfair under the FTCA, the FTC looks to the three elements of the unfairness test to see if the act or practice "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition."[121] If the FTC files an action against Target, the company's conduct leading up to the data breach will be subject to the unfairness test. Applying the three factors of the unfairness test will likely weigh in favor of a determination that Target engaged in an unfair act or practice by failing to take action when its security system detected the breach.

Unlike LabMD, which lacked any sort of computer security safeguards, Target had a security system that detected the malware stealing consumer credit card information and subsequently issued warnings to Target.[122] Despite these notifications, Target took no action, thereby allowing the malware to spread into its computer system.[123] Target's omission appears comparable to the situation in *Wyndham Worldwide Corp.*, where the company failed to take action to prevent any further data breaches following an initial breach, thereby allowing the hackers to have continued unauthorized access to the data.[124]

A. Substantial Injury to Consumers

Under the FTCA, a "substantial injury" usually involves a monetary harm; "[e]motional impact and other more subjective types of harm" will not render a practice unfair.[125] Furthermore, although the FTC "is not concerned with trivial

---

119. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) ("The committee gave careful consideration to the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce . . . It concluded that . . . there were too many unfair practices to define, and after writing [twenty] of them into the law it would be quite possible to invent others." (quoting S. REP. NO. 63-597, at 13 (1914))); FTC v. Sperry Hutchinson Co., 405 U.S. 233, 239–40 (1972).

120. "The takeaway is that Congress designed the term as a 'flexible concept with evolving content,' FTC v. Bunte Bros., 312 U.S. 349, 353 (1941), and 'intentionally left [its] development . . . to the [FTC],' Atl. Ref. Co. v. FTC, 381 U.S. 357, 367 (1965)." *Wyndham Worldwide Corp.*, 799 F.3d at 243 (alteration in original).

121. *LabMD, Inc.*, 2014 F.T.C. LEXIS 2, at*11 (F.T.C. Jan. 16, 2014) (alteration in original) (quoting 15 U.S.C. § 45(n)).

122. WEISS & MILLER, *supra* note 1, at 2. On November 12, 2013, the hackers breached Target's computer system. "The intrusion was detected by Target's security systems, but the company's security professionals took no action . . . ." *Id.* (citing the testimony of John J. Mulligan, Executive Vice President and Chief Financial O fficer of Target).

123. *Id.*

124. *Wyndham Worldwide Corp.*, 799 F.3d at 242.

125. *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter *Policy Statement*]. Examples of monetary harms include "when sellers coerce consumers into purchasing unwanted

or merely speculative harms,"[126] it recognizes that an injury may be substantial based on the number of people affected or the overall significance of the risk of harm.[127]

In *LabMD, Inc.*, the company argued that the FTC "lack[ed] authority to apply the FTC Act's prohibition of 'unfair . . . acts or practices' to data security practices," but this contention was wholly rejected by the Commission.[128] When considering LabMD's conduct in light of the first factor of the unfairness test, causation or likely causation of substantial injury to consumers, the FTC argued that LabMD collected and stored "highly sensitive information on consumers' identities," while "implement[ing] unreasonable data security measures."[129] Furthermore, LabMD failed to utilize any "readily-available safeguards" to protect its computer system from hacker activity.[130] A billing manager even installed Limewire, a peer-to-peer file-sharing program, on a company computer, which increased the risk of third party invasion into LabMD's computer system.[131]

These acts and omissions, the FTC alleged, were direct causes of the data breach that enabled "unauthorized persons to obtain sensitive consumer information," as well as increased the threat of other potential breaches.[132] The actual and potential data breaches caused substantial injury to consumers by exposing their personal information, including Social Security numbers and addresses, to unauthorized persons. LabMD's actions were also likely to cause substantial injury to consumers as the breach increased the risks of identity theft, medical identity theft, and exposure of "sensitive private medical information."[133]

In *Wyndham Worldwide Corp.*, Wyndham argued that the three requirements of the FTC's unfairness test were "insufficient conditions of an unfair practice,"[134] and that, even if the test was intended to cover cybersecurity, the

---

goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction. Unwarranted health and safety risks may also support a finding of unfairness." *Id.* (footnotes omitted); *see, e.g.*, Holland Furnace Co. v. FTC, 295 F.2d 302, 305 (7th Cir. 1961) (holding a seller's dismantling of furnaces and then refusing to reassemble them until the consumer agreed to pay for services or replacement parts constituted an unfair act under the FTCA); *see also*, Preservation of Consumers' Claims and Defenses, 40 Fed. Reg. 53,506, 53,522–23 (Nov. 18, 1975) (to be codified at 16 C.F.R. pt. 433).

126. *Policy Statement*, *supra* note 125.

127. *Id.* at n.12 ("An injury may be sufficiently substantial, however, if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm.").

128. LabMD, Inc., 2014 F.T.C. LEXIS 2, at *39 (F.T.C. Jan. 16, 2014).

129. *Id.* at *51.

130. *Id.*

131. *Id.*

132. *Id.* at *51–52.

133. *Id.* at *51, *53–54.

134. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244 (3d Cir. 2015).

FTC still lacked authority over such practices.[135] However, the court rejected these arguments and held that Wyndham's data security failures constituted an unfair act or practice under the FTCA, thereby affirming the FTC's enforcement powers.[136] As a result of the data breaches, the payment account information of millions of consumers was compromised, with considerable harm caused to those consumers who fell victim to identify theft.[137]

To defend against the FTC's charge that its conduct caused or was likely to cause substantial injury to consumers, Wyndham asserted that it could not have treated its customers unfairly if the corporation itself was "victimized by criminals."[138] Under this theory, Wyndham could not be at fault for the substantial injury to consumers because the breaches harmed Wyndham as well. Wyndham ultimately argued that its failure to prevent data breaches—an omission rather than an act—could not support a finding that the corporation, in fact, engaged in unfair conduct. Accordingly, the harm to consumers was directly caused by the hackers, not by what Wyndham itself had done.[139]

Even though the Third Circuit acknowledged that unfairness actions "usually involve actual and completed harms,"[140] the court posited that the FTCA "expressly contemplates the possibility that conduct can be unfair before actual injury occurs."[141] Still, Wyndham defended against the charges of unfairness by highlighting that the actions of a third party, which carried out the three cybersecurity attacks that resulted in the subsequent data breaches, were, in fact, the direct cause of the substantial injury to consumers.[142] The Third Circuit, however, rejected Wyndham's defense by reasoning that, although Wyndham's failure to implement adequate data security measures "was not the most proximate cause of an injury," this fact did not immunize the corporation from liability for foreseeable harms.[143] Accordingly, the court found that where

---

135. *Id.* at 246 ("[I]f the FTC's unfairness authority extends to Wyndham's conduct, then the FTC also has the authority to 'regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door.'" (quoting Appellant's Opening Brief at 23, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015) (No. 14-3514))).

136. *Id.* at 259.

137. *Id.* at 242 ("[C]onsumers suffered financial injury through 'unreimbursed fraudulent charges, increased costs, and lost access to funds or credit,' and that they 'expended time and money resolving fraudulent charges and mitigating subsequent harm.'" (citation omitted)).

138. *Id.* at 246.

139. *Id.*

140. *Id.* (quoting Int'l Harvester Co., 104 F.T.C. 949, 1061 (1984)).

141. *Id.* (citing 15 U.S.C. § 45(n) (2012)).

142. *Id.* at 245–246.

143. *Id.* at 246; *see* RESTATEMENT (SECOND) OF TORTS § 449 (AM. LAW INST. 1965) ("If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby."); *see also* Westfarm Assocs. Ltd. P'ship v. Wash. Suburban Sanitary Comm'n, 66 F.3d 669, 688 (4th Cir. 1985) ("Proximate cause can may be found where the conduct of the third party is tortious or

harmful actions of a third party result from a company's own failures, that can be sufficient to subject the company to liability.[144]

Moreover, despite the fact that these data security intrusions were foreseeable, Wyndham failed to restrict access to its network and did not utilize appropriate measures to prevent unauthorized access into its computer system, amongst other cybersecurity failures.[145] As a result, Wyndham knew, or should have known, that its lack of data security precautions could result in a data breach.[146] Therefore, Wyndham's data security failures caused, and were likely to cause, substantial injury to consumers, satisfying the first element of the unfairness test.

As a result of the Target breach, the payment account numbers and other sensitive information of millions of consumers were stolen.[147] Many of these consumers also incurred monetary harms when they experienced fraudulent activity on debit and credit cards they used at Target.[148] Additionally, these harms not only exposed the sensitive information of a large number of people; they also created a significant risk of fraud to millions of consumers whose payment information was in Target's computer system.[149] The malware that spread through Target's system was able to capture the card information and PIN numbers of customers, exposing them to the possibility of having their PII compromised.[150] These factors are evidence of a substantial injury to consumers and resulted from the breach that occurred because of Target's unfair data security practices.

In the *LabMD, Inc.* case, the substantial injury that resulted from the laboratory's unfair acts or practices was the exposure of sensitive personal information of consumers, which increased likelihood of identity theft.[151] Similarly, in *Wyndham Worldwide Corp.*, the substantial injury to consumers was the compromise of their payment account information and the subsequent

---

criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable.").

144. *Wyndham Worldwide Corp.*, 799 F.3d at 246.

145. *Id.* at 256.

146. *Id.*

147. WEISS & MILLER, *supra* note 1, at 2. The Target breach exposed the sensitive information of millions of consumers, but not every consumer will be affected because the hackers did not use every piece of data it encountered. Furthermore, some cards were canceled before the hackers could use them, and other attempts to use valid cards were denied by the issuing financial institutions. *Id.* Although the breach did not impact every Target customer, it may still constitute a substantial injury because it imposed "a small harm to a large number of people" and raised "a significant risk of concrete harm" to those customers whose confidential information was exposed to the hackers. *See Policy Statement*, *supra* note 125, at n.12.

148. WEISS & MILLER, *supra* note 1, at 2–3.

149. The malware captured payment card information before it became encrypted, which would have made it more difficult to read. Allegedly, the "malware known as a 'memory scraper' captured information from customers' payment cards by reading the POS system's memory before it was encrypted." *Id.*

150. *Id.* at 2.

151. LabMD, Inc., 2014 F.T.C. LEXIS 2, at *52–54 (F.T.C. Jan. 16, 2014).

identity theft.[152] In the Target breach, the payment information of consumers was exposed, not only increasing the possibility of identity theft but also causing many consumers to experience fraudulent card activity.[153] Harms similar to those in *Target* were found to be substantial injuries in both *LabMD, Inc.* and *Wyndham Worldwide Corp.*, so it is likely that the FTC would find that a substantial injury to consumers occurred from the Target breach.

Moreover, the court in *Wyndham Worldwide Corp.* asserted that the corporation's conduct caused substantial injury to consumers because the data security intrusions were foreseeable.[154] Wyndham should have been aware that potential data breaches could occur due to inadequate security, especially after experiencing two breaches.[155] Similarly, despite the fact that Target received notice of a breach, it initially took no action to prevent further intrusions.[156] Thus, like the foreseeability of the data breaches in *Wyndham Worldwide Corp.*, Target should have foreseen the subsequent and more extensive breach because it was aware of the initial intrusion.[157]

B. Reasonable Avoidability by Consumers

The second element of the unfairness test is that the substantial injury to consumers caused by the unfair act or practice was "not reasonably avoidable by consumers themselves."[158] Under this notion, the FTC relies on "the ability of individual consumers to make their own private purchasing decisions without regulatory intervention."[159]

However, consumers whose personal information was stored on LabMD's computer system had no prior knowledge of the corporation's data security issues.[160] As a result, there was little they could have done to avoid the harm that ensued from the breach.[161] If consumers were unaware of LabMD's security failures—and probably unaware of LabMD's existence—it is not reasonable to expect them to be able to avoid the substantial harm caused by

---

152. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

153. WEISS & MILLER, *supra* note 1, at 2.

154. *Wyndham Worldwide Corp.*, 799 F.3d at 246.

155. *Id.* at 256.

156. WEISS & MILLER, *supra* note 1, at 2–3.

157. *Id.*

158. 15 U.S.C. § 45(n) (2012).

159. *Policy Statement*, *supra* note 125.

> Normally we expect the marketplace to be self-correcting . . . . We anticipate that consumers will survey the available alternatives, choose those that are most desirable, and avoid those that are inadequate or unsatisfactory. However, it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary. Most of the [FTC]'s unfairness matters are brought under these circumstances.

Id.

160. LabMD, Inc., 2014 F.T.C. LEXIS 2, at *54–55 (F.T.C. Jan. 16, 2014).

161. *See id.*

such failures. Therefore, the substantial injury to consumers in the case of *LabMD* satisfies the second element of the unfairness test because such harm was not reasonably avoidable by consumers.

Likewise, in the case of *Wyndham Worldwide Corp.*, consumers could not have reasonably avoided the substantial harm caused by the data breaches when Wyndham, itself, was unaware of the attacks.[162] Wyndham was unaware of the attacks for two months following the second breach until consumers complained about fraudulent charges on their accounts.[163] Additionally, Wyndham remained unaware of the third attack until cardholders complained to a credit card company.[164] If Wyndham had no knowledge of the breaches until consumers had already been harmed, it is likely that consumers were unaware of any of Wyndham's data security failures. Due to this lack of insight, consumers could not have reasonably avoided the substantial harm from the breaches.

Similarly, the injuries suffered by consumers following the Target breach were not reasonably avoidable. Nothing in the normal act of swiping a credit or debit card would indicate to customers that their information was being captured, and Target did not notify the public of the breach until a month after it occurred.[165] Millions of consumers shop at Target, frequently using their debit or credit cards to make purchases.[166] Consumers could not have avoided their injuries, as they had no way of expecting their payment information to be exposed.[167] Furthermore, Target had not previously been subject to a mass breach, so consumers had no reason to expect it to occur.[168] As a result, the harm caused by the breach was not reasonably avoidable by the consumer.[169]

C. Countervailing Benefits

Third, to constitute an unfair act or practice, there must not be any "countervailing benefits to consumers or to competition" that outweigh the injury suffered.[170] A substantial injury can be, in some cases, "outweighed by

---

162. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242, 246 (3d Cir. 2015).

163. *Id.* at 242.

164. *Id.*

165. WEISS & MILLER, *supra* note 1, at 2–3. Target itself was unaware of the breach until it was notified by the Department of Justice, and did not make a public announcement until after meeting with the Department of Justice and the U.S. Secret Service. *Id.* at 3.

166. *Id.* at 2.

167. *Id.* (noting that consumer information was compromised before Target even had the opportunity to encrypt their data).

168. *Id.* Notably, this is distinguished from Wyndham's three breaches. Unlike Wyndham, Target received warnings when the malware that led to the harm breached its computer system. Cf. *Wyndham Worldwide Corp.*, 799 F.3d at 255–56.

169. Target did not make a public announcement until December 19, 2013—an entire month after the breach. Therefore, consumers could not have known that their information would be compromised if they shopped at Target. *See* WEISS & MILLER, *supra* note 1, at 2–3.

170. 15 U.S.C. § 45(n) (2012).

any offsetting consumer or competitive benefits that the sales practice also produces."[171] The FTC will not conclude that a practice unfairly injures consumers "unless it is injurious in its net effects."[172] Furthermore, the FTC will also take into account the costs of remedying the injury.[173]

In *LabMD*, the breach not only injured consumers, but LabMD suffered harm as well when the hackers accessed the computer system without LabMD's consent.[174] Because the infringement on sensitive computer files both exposed consumers to an increased risk of theft and invaded LabMD's infrastructure,[175] any countervailing benefit must clear a substantial hurdle to outweigh the injury suffered. Furthermore, because LabMD could have prevented potential data breaches "at a relatively low cost" by investing in an efficient cybersecurity system,[176] these factors show that there were scant, if any, countervailing benefits to the cyber invasion and, thus, weigh in favor of a finding of unfairness.

To determine whether or not countervailing benefits outweighed the harms caused by the breaches in *Wyndham Worldwide Corp.*, the Third Circuit performed a cost-benefit analysis of the cost to consumers in preventing such a breach, and the probability of the harm given that level of cybersecurity.[177] However, as the court points out, the FTC did not allege that Wyndham's data security practices were *weak*, but rather, that Wyndham failed to use *any* data security measures *at all*.[178] Wyndham, in turn, offered no response to this allegation in its reply brief.[179] Moreover, Wyndham's computer system was hacked a total of three times, so it should have recognized after the first, or even the second, breach that harm to consumers was highly likely given its lack of

171. *Policy Statement*, *supra* note 125 ("Most business practices entail a mixture of economic and other costs and benefits for purchasers. A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article.").

172. *Id.* When determining the presence of countervailing benefits, "the [FTC] may refer to existing public policies for help in ascertaining the existence of consumer injury and the relative weights that should be assigned to various costs and benefits." *Id.*

173. Such remedies include "not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters." *Id.*

174. LabMD, Inc., 2014 F.T.C. LEXIS 2, at *50–51.

175. *Id.*

176. *Id.* at *55.

177. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2015).

178. *Id.* at 256 ("[T]he complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all*." (citations omitted)).

179. *Id.*

cybersecurity measures.[180] Wyndham's data security failures, and the subsequent harm caused, should have led Wyndham to implement preventive measures. Wyndham's lack of response showed that its conduct failed the cost-benefit analysis.

Following the Target breach, consumers faced fraudulent charges and endured expenses when they were forced to open new payment accounts.[181] These "net effects" of the breach add to the injury and do not provide any offsetting benefits to consumers.[182] Nor were there any offsetting competitive benefits to Target following the breach, as the corporation faced multiple class action lawsuits and will potentially be subject to FTC action.[183] Furthermore, under a cost-benefit analysis like the one in *Wyndham Worldwide Corp.*,[184] Target should have recognized the increasing probability of harm facing its consumers with its insufficient cybersecurity measures given that it received early notice of the data breach.[185] Thus, because Target, like Wyndham, failed to take any corrective action, its conduct fails the cost-benefit analysis.

The absence of countervailing benefits to consumers and competition following the Target breach have satisfied the requirements of a substantial injury under the unfairness test.[186] As Target's conduct meets all three elements of the unfairness test, it is likely that the FTC would succeed in an action against Target. However, in absence of express authority to take enforcement action against data breaches, Target could potentially succeed in challenging the FTC's enforcement powers in this realm.

III. FEDERAL LEGISLATION COULD GRANT THE FTC THE POWER IT NEEDS

Although the FTC has successfully maintained its authority under Section 5 to take enforcement action against data breaches, the FTC itself has emphasized to Congress the importance of enhanced federal data security legislation.[187] With the express power to take enforcement action against data breaches, entities that fall victim to breaches, such as Target, would not be able to challenge the FTC's enforcement authority in matters of cybersecurity. Accordingly, legislators have made efforts to address this issue.

---

180. *Id.* at 255–56 ("[Wyndham] was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis.").

181. *See* WEISS & MILLER, *supra* note 1, at 6.

182. Payment networks have issued claims against Target for reimbursement of incremental expenses, such as fraudulent losses and card reissuance. *Id.*

183. *See id.* (reporting that Target incurred $248 million in expenses related to the data breach and received $90 million from insurance policies in November 2014).

184. *See supra* notes 177–80 and accompanying text.

185. *See supra* notes 122–24 and accompanying text.

186. *See* 15 U.S.C. § 45(n) (2012) (codifying the three-factored unfairness test).

187. Ramirez, *supra* note 2, at 14 (calling for the "enactment of a strong Federal data security and breach notification law").

The proposed Data Breach Notification and Punishing Cyber Criminals Act of 2015 (the Bill) would specifically require entities to "take reasonable measures to protect and secure data in electronic form containing personal information."[188] Under this proposal, an entity that fails to take such reasonable measures would be subject to FTC authority, and the entity's failure "shall be treated as an unfair or deceptive act or practice."[189] By expressly granting data security enforcement powers to the FTC,[190] this Bill would eliminate any challenges that Target could raise surrounding the FTC's authority to take action in such situations.[191]

A. Necessary Enhancements to the Data Breach Notification and Punishing Cyber Criminals Act of 2015

The increasing frequency of mass data breaches implores the passing of data security legislation to minimize the risk of such invasions.[192] The Bill, if enacted, would set forth the authority the FTC needs to continue taking enforcement action in data breach cases.[193] However, to ensure that companies put effective data security measures in place, Congress should send a clear and unequivocal message that failure to implement a data security policy, or failure to take corrective measures after a data breach has occurred, will result in increased liability for any subsequent breaches.

This means that once an entity's data is breached, irrespective of culpability, the entity should be per se liable for any subsequent breach that occurs. Furthermore, once the entity is held per se liable for subsequent breaches, it should be prohibited from contesting the FTC's authority in the matter. The presence of such language in the Bill would prevent entities from challenging the FTC's ability to bring such an action in the first place.

Moreover, such a rule would surely encourage all entities that handle consumer data to implement adequate data security measures, thereby preventing the problem of invasion of easily-accessed computer systems. It would also accomplish the public policy goal of protecting consumer

---

188. Data Breach Notification and Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. § 2 (2015). This bill not only mandates reasonable data security, it also requires covered entities to notify affected consumers once an information security breach has occurred. *Id.* § 3.

189. *Id.* § 4(c)(1).

190. *See id.* § 4(c)(2).

191. *See* Ramirez, *supra* note 2, at 20 ("Legislation in both areas—data security and breach notification—should give the FTC the ability to seek civil penalties to help deter unlawful conduct . . . . To help ensure effective deterrence, [the FTC] urge[s] Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances.").

192. *See id.* at 16 (stating that the FTC's policy goals "to protect consumer privacy and promote data security in the private sector" would be served through the passing of federal legislation).

193. *See Protecting Personal Consumer Information from Cyber Attacks and Data Breaches: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 113th Cong. 16 (2014) (statement of Hon. Edith Ramirez, Chairwoman, Fed. Trade Comm'n) ("The FTC remains committed to promoting reasonable security for consumer data . . . .").

information under the FTCA. This per-se liability rule, however, should only apply six months after the occurrence of the breach, thereby allowing the affected entity to implement adequate data security measures.

Through amendments to the Bill, Congress should also grant the FTC the authority to promulgate rules and regulations for general data security practices.[194] Rulemaking authority, in accordance with the procedures established by the Administrative Procedure Act,[195] would allow the FTC to require companies to implement specific data security measures.[196] Having the express authority to set requirements for companies' data security "would allow the FTC to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data."[197]

IV. CONCLUSION

In light of the many mass data breaches that have occurred recently, there is a need for enhanced federal data security legislation. The FTC has become the lead enforcer in federal data breach cases under the notion that entities with data breaches may have engaged in an unfair act or practice under the FTCA through inadequate security measures. However, as the FTC has continued using its Section 5 power broadly, it is receiving more questions as to whether its authority extends to data breaches. Although courts have upheld the FTC's Section 5 authority against such challenges, the FTC would benefit from federal legislation expressly providing it with data security enforcement power.

The proposed Data Breach Notification and Punishing Cyber Criminals Act of 2015, if enacted, will enhance cybersecurity efforts by authorizing the FTC to take action against those companies, such as Target, that fail to take reasonable measures to protect against data breaches. However, to further enhance cybersecurity practices, the Bill should be amended to specifically state that an entity that is subject to a data breach will be held liable to the FTC for any subsequent breaches that may occur, and that the FTC has rulemaking authority in the general data security context. By expressly granting the FTC rulemaking authority for general data security practices, the Bill assists the FTC

194. *See* Ramirez, *supra* note 2, at 20–21.

195. 5 U.S.C. § 553 (2012).

196. *See* Ramirez, *supra* note 2, at 20–21 ("[R]ulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology.").

197. *Id.* at 21.

> For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years, a child's Social Security number alone can be used in combination with another person's information, such as name or data of birth, in order to commit identify theft.

Id.

in encouraging the implementation of readily available data protection measures, thereby preventing future data breaches.