Buffalo Law Review

Volume 67 | Number 4 Article 4

8-1-2019

The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America

Gregory S. Gaglione Jr.
Buffalo Law Review

Buffalo Law Review

VOLUME 67 AUGUST 2019 NUMBER 4

The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America

GREGORY S. GAGLIONE, JR.†

INTRODUCTION

"Identity theft is not a joke, Jim! Millions of families suffer every year!"[1] Although this statement by Dwight Schrute in an episode of *The Office* was intended to be a joke, given the recent rise in data breaches, it is a reality to many Americans today. A combined 200 million individuals were affected by the Equifax and Uber data breaches alone in 2017.[2] In total, over 2.5 billion records were compromised in

†J.D., 2019, University at Buffalo School of Law; M.B.A., 2019 University at Buffalo School of Management; B.A., Economics, 2015, University at Buffalo; Publications Editor, *Buffalo Law Review*; Certified Information Privacy Professional/United States. I am grateful for my colleagues at the Buffalo Law Review for their time and effort editing this Comment. Special thanks goes to my family and friends for their support and encouragement, especially my fiancé Theresa Johnson. Without their love and support, this Comment would not be possible.

1. *The Office: Product Recall* (NBC television broadcast April 26, 2007).

2. *See* Mike Isaac et al., *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/uber-hack.html; Equifax Inc., *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 [hereinafter EQUIFAX].

publicly disclosed data breaches in 2017.[3] That number is likely to increase in 2018 due to the massive data breaches at Facebook[4], Marriott[5], and Under Armour.[6] However, even though there has been a substantial increase in data breaches over the past few years,[7] the legal system has not evolved to provide protections for consumers.

Currently, circuit courts are divided over whether the risk of future harm that data breach victims incur is enough to establish an injury-in-fact for Article III standing.[8] Additionally, in 2018, Alabama and South Dakota became the final two states to pass a data breach notification law.[9]

---

3. *See* GEMALTO, FINDINGS FROM THE 2017 BREACH LEVEL INDEX 2, GEMALTO (2018), https://blog.gemalto.com/security/2018/04/13/data-breach-stats-for-2017-full-year-results-are-in/ (stating that over 2.5 billion records were breached in 2017, which is up 88% from 2016).

4. Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html. Facebook announced in September that "an attack on its computer networked exposed the personal information of nearly 50 million users."

5. Seena Gressin, *The Marriott data breach*, F.T.C. (Dec. 4, 2018), https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach. Marriott International announced in November 2018 that a breach of its guest reservation database exposed the personal information of up to 500 million people.

6. Lisa Marie Segarra, *Under Armour Data Breach Exposes 150 Million MyFitnessPal Accounts*, TIME (Mar. 30, 2018), http://time.com/5222015/under-armour-myfitnesspal-data-breach/. In March 2018 Under Armour announced that there was a security breach with Under Armour's MyFitnessPal system affecting 150 million users.

7. *See* Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds*, NBC NEWS (July 24, 2017), https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881.

8. Dominic Spinelli, *Data Breach Standing: Recent Decisions Show Growing Circuit Split*, ABA (January 26, 2018), https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/data_breach_standing_recent_decisions_show_gowing_circuit_court_split/. *See also* Bradford C. Mank, *Data Breaches Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1328 (2017) (advocating for the Supreme Court to address this circuit split).

9. *See* EMILY WESTRIDGE BLACK ET AL., *Key Features of New Data Breach Notification Laws in Alabama and South Dakota*, 4(5) PRATT'S PRIVACY AND

With these two new data breach notification statutes, there are now fifty separate state data breach notification laws.[10] These laws differ in complexity and severity, making it difficult for companies to comply with all fifty notification statutes when a breach occurs.[11] As a result, many data breach victims are completely unaware that their personal information is in the hands of hackers because either their state data breach notification law is not strict enough, or a company simply has failed to comply with the state law and notify all the individuals involved in the breach.[12] In short, the law currently does not offer the proper protections for

---

CYBERSECURITY LAW REPORT 139, 147 (2018).

10. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [hereinafter NCSL](providing a list of all fifty state data breach notification laws).

11. Bart A. Lazar, *Security Breach Responses: As Important and Difficult as Ever*, CYBER L. & STRATEGY (June 8, 2018) at 6 (explaining the material differences in notification statutes including "the definition of personal information covered by the statute; the definition of a breach; exceptions for providing notice because of the lack of materiality or risk of harm associated with the breach; whether and to the extent encrypted data is exempted from a breach; timing requirements for providing notice to individuals; the contents of a notice;" etc. The many material differences between the notification statutes creates "confusion and the unnecessary expenditure of time and resources figuring out a company's responsibilities, battles between companies and their service providers about whether a notification should be sent, who sends notifications, the content of the notification and when the notifications should be sent.").

12. *See* Nicole Lyn Pesce, *An Alarming Number of People Still Don't Know if They Were Hurt by the Equifax Hack*, MKT. WATCH (July 25, 2018), https://www.marketwatch.com/story/an-alarming-number-of-people-still-dont-know-if-they-were-hurt-by-the-equifax-hack-2018-07-25; Paul Roberts, *For U.S. Consumers: Ignorance of Data Breaches is Bliss*, DIGITAL GUARDIAN (Dec. 21, 2017), https://digitalguardian.com/blog/us-consumers-ignorance-data-breaches-bliss (explaining that the "U.S. lacks a comprehensive, federal data privacy and data protection law that compels firms to notify consumers when their information has been compromised" and the many state data breach notification laws does not provide a uniform standard, which makes the likelihood of learning of the theft of one's information dependent in part on where one lives); Octavio Blanco, *Millions of Consumers Still Unaware of Equifax Data Breach*, CONSUMER REPORTS (Nov. 9, 2017), https://www.consumerreports.org/consumer-protection/millions-of-consumers-still-unaware-of-equifax-data-breach/.

consumers once their personal information has been hacked.

The recent Equifax data breach in 2017 showcased the current cybersecurity problems in America today. This Comment will focus on the Equifax data breach and discuss the opportunity it presents to improve consumer protection and cybersecurity efforts in America. The Comment will argue for two fundamental changes to be made in American law. The first change requires action by the United States Supreme Court. The Supreme Court can use the Equifax data breach as an opportunity to clarify the current circuit split surrounding Article III standing for data breach class action cases. This Comment argues that the Supreme Court should follow the D.C., Sixth, Seventh, and Ninth Circuit Courts' recent rulings that allow for standing in a data breach case based on the risk of future harm.[13] The second change in the law requires action from the United States Congress. This Comment proposes that Congress pass a federal privacy law that will protect consumer personal information and provide penalties for organizations that violate the law and harm consumers by putting their data at risk. These two changes in the law will act as general and specific deterrents for companies that fail to protect their customers' personal information.[14] With these laws in place as a deterrent, they will shape companies' behavior to improve cybersecurity efforts that will then prevent future data breaches. In sum, these two changes to the law will incentivize organizations to improve their cybersecurity efforts and allow for better consumer protection before and after a data breach occurs.

Part I of this Comment provides a historical background of data breaches, highlighting the prominent security breaches that occurred prior to 2019. Part II explains the

13. *See* Lee J. Plave & John W. Edson, *First Steps in Data Privacy Cases: Article III Standing*, 37 FRANCHISE L.J. 485, 485, 487 (2018).

14. *See* BRIAN T. FITZPATRICK, *Do Class Actions Deter Wrongdoing?*, *in* THE CLASS ACTION EFFECT (Catherine Piché, ed., Éditions Yvon Blais, Montreal, 2018).

harmful effects data breaches have on companies, consumers, and the economy as a whole. Part III provides an in-depth evaluation of the Equifax data breach and how it provides an opportunity for America to learn from the breach to improve consumer protection and cybersecurity efforts. Part IV details the current circuit split regarding Article III standing in data breach class action cases, as well as an overview of the privacy laws enacted recently in the United States and abroad. Finally, Part V offers a proposed solution including both the Supreme Court addressing the circuit split and Congress passing a federal privacy law to improve consumer protection and cybersecurity efforts in America.

I. HISTORICAL BACKGROUND OF DATA BREACHES

The Cambridge Dictionary defines a data breach as "an occasion when private information can be seen by people who should not be able to see it."[15] Under this definition, the first recorded data breach, arguably, occurred in the Garden of Eden when Adam and Eve gained unauthorized access into the Tree of Knowledge of Good and Evil by eating an apple from the tree against God's command.[16] The legal definition of a data breach is "the loss, theft, or other unauthorized access . . . to data containing sensitive personal information, in electric or printed form, that results in the potential compromise of the confidentiality or integrity of the data."[17] Still, under this definition, data breaches did not originate when companies began storing their data digitally. Before computing was commonplace, a data breach could constitute something as simple as viewing an individual's medical file without authorization or finding sensitive documents that

15. *Data Breach*, CAMBRIDGE DICTIONARY https://dictionary.cambridge.org/us/dictionary/english/data-breach (last visited Feb. 26, 2019). In this Comment the terms "data breach" and "security breach" are used interchangeably.

16. *See Genesis* 3:1–14.

17. 38 U.S.C. § 5727(4).

were not properly discarded.[18] However, these pre-digital age data breaches were not nearly as prevalent as the data breaches seen today. Once data became digitized and stored in large quantities, data breaches became much more rampant.

The advent of the internet and the digital age has made data[19] more valuable than ever.[20] Organizations now gather large amounts of customer personal information and use this information as an integral part of their business strategy.[21] At the same time, technological advancement also made it easier for cybercriminals to hack into an organization's system.[22] Indeed, as electronic data storage increased in the

---

18. David F. Perri & Erinmichelle D. Perri, *Acknowledging the "M" in MIS: Managing a Data Breach Crisis*, 19 J. OF THE ACAD. OF BUS. 9, 11 (2018).

19. Data is customer information for the purposes of this Comment. Data and personal information are used interchangeably throughout this Comment.

20. *See The World's Most Valuable Resource is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. *See also* James Grottola, *Data is the World's Most Valuable Resource*, RINGLEAD (Dec. 4, 2017), https://www.ringlead.com/blog/data-is-the-worlds-most-valuable-resource/ (explaining why data is valuable in the business environment and the importance of protecting data).

21. James Grottola, *Data is the World's Most Valuable Resource*, RINGLEAD (Dec. 4, 2017), https://www.ringlead.com/blog/data-is-the-worlds-most-valuable-resource/ (claiming that 97 percent of businesses use data to power their business opportunities and 76 percent of businesses use data as an integral part of forming a business strategy); *see also* Adam C. Uzialko, *How Businesses Are Collecting Data (And What They Are Doing with It)*, BUS. NEWS DAILY (Aug. 3, 2018), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (explaining that consumer data is often used by companies to improve their marketing strategy and customer experience. Some companies even collect data simply to sell to other companies).

22. *See* Andrew Rossow, *Why Data Breaches Are Becoming More Frequent and What You Need to Do*, FORBES (May 23, 2018, 3:12 PM), https://www.forbes.com/sites/andrewrossow/2018/05/23/why-data-breaches-are-becoming-more-frequent-and-what-you-need-to-do/#570d20bcd97f; *see also* Juliana De Groot, *The History of Data Breaches*, DIGITAL GUARDIAN (Jan. 3, 2019), https://digitalguardian.com/blog/history-data-breaches. (explaining the four most common types of data breaches: ransomware, malware, phishing, and denial-of-service, all four of which use computer software to hack into computer systems).

1980s and 1990s, it inevitably led to more data breaches. As the world's volume of data has been growing exponentially year after year, it has given cybercriminals "a greater opportunity to expose massive amounts of data in a single breach."[23] Therefore, with data more valuable than ever and technological innovation at an all-time high, cybercriminals[24] now have the technological ability and a monetary incentive to hack into an organization's information system and steal the personal information of millions of Americans.[25]

The first reported digital data breach was the AOL data breach in 2004, where a twenty-four-year-old AOL employee stole 92 million customer email addresses and screen names with the intention of selling the information to bulk emailers.[26] As a result, AOL users received excess spam from those who had purchased their emails and usernames.[27] Around the same time as the AOL breach, public awareness of the potential for data breaches began to rise. Consequently, Privacy Rights Clearinghouse,[28] a non-profit

---

23. De Groot, *supra* note 22.

24. In this Comment, "cybercriminals" and "hackers" are used interchangeably.

25. *See* Vivek Sharma, *Why Do Data Breaches Happen?*, USC MARSHALL SCH. OF BUS. (Sept. 25, 2017), https://www.marshall.usc.edu/blog/why-do-data-breaches-happen. (explaining that after a massive data breach, cybercriminals will sell the stolen data to other criminals who will use it to make fraudulent purchases).

26. Davis Stout, *AOL Engineer Sold 92 Million Names to Spammer, U.S. Says*, N.Y. TIMES (June 23, 2004), https://www.nytimes.com/2004/06/23/technology/aol-engineer-sold-92-million-names-to-spammer-us-says.html. *See also* Meg Krafft, *A Brief History of Data Breaches*, THE SEC. AWARENESS CO. (Mar. 6, 2018), https://www.thesecurityawarenesscompany.com/2018/03/06/brief-history-data-breaches/.

27. Krafft, *supra* note 26. Luckily, passwords and credit card numbers were not breached, leaving this data breach less harmful than the Equifax data breach and others that have occurred recently.

28. Privacy Rights Clearinghouse is a 501(c)(3) nonprofit organization protecting privacy for all by empowering individuals and advocating for positive

organization advocating for privacy protection, began recording and gathering information on data breaches in 2005.

The year 2005 also became infamous as the year of the first data breach to compromise more than 1 million records when DSW Shoe Warehouse had 1.4 million credit card numbers and names on accounts hacked.[29] In the same year, the first data breach to affect a college campus occurred when George Mason University was breached in January of 2005 where names, pictures, and Social Security numbers of 32,000 students and staff were exposed to hackers.[30]

Since 2005, data breaches have become larger and more dangerous with each passing year. Accordingly, in 2009, the first breach to involve over 100 million records was recorded when Heartland Payment Systems experienced a breach that exposed 130 million credit card accounts.[31] Following the Heartland breach, data breaches continued to reach new heights. In 2013, Target was involved in a highly-publicized

---

change. Clearinghouse, *About Privacy Rights Clearinghouse,* PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/about. In total, Privacy Rights Clearinghouse reports that there have been over 11 billion records breached from over 9,000 data breaches made public from 2005 to 2019. Clearinghouse, *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches (last visited Jan. 4, 2019).

29. Symantic Corporation, *A Brief History of Data Breaches*, LIFELOCK (2018), https://www.lifelock.com/education/history-of-data-breaches/ [hereinafter LIFELOCK]. *See generally* Clearinghouse, *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches?title=&taxonomy_vocabulary_11_tid%5B%5D=271 (last visited Jan. 4, 2019) (listing all of the significant data breaches in 2005 and the relevant information regarding each breach).

30. LIFELOCK, *supra* note 29. *See also* Clearinghouse, *Data Breaches by Organization Type*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches/organization?taxonomy_vocabulary_11_tid=2434 (last visited Jan. 4, 2019) (providing information on each organization affected by a data breach, including the education sector which represents a significant portion of organizations affected by a data breach each year).

31. *Data Breaches by Organization Type*, *supra* note 30. *See also Data Breaches*, *supra* note 29. (providing the pertinent information regarding the Heartland Payment Systems data breach in 2009).

data breach where 110 million individuals' payment and contact information were exposed.[32] However, the Target breach was not even the largest breach of 2013. Yahoo! took the crown as the largest data breach in that year when it experienced a breach exposing over 3 billion user accounts.[33] Yahoo! initially discovered the breach in September 2016 and disclosed that 500 million accounts were hacked in 2014. After further review, Yahoo! announced that an initial breach occurred in 2013 and affected 1 billion user accounts. Finally, in 2017 Yahoo! revised that estimate and acknowledged that the breach actually exposed all 3 billion user accounts within Yahoo!. Yahoo!'s security breach exposed the names, dates of birth, email addresses, passwords, security questions and answers of its users. To date, the Yahoo! data breach is the largest data breach in the United States.[34]

Data breaches gained more fame when a breach affected high-profile Hollywood actors, actresses, and executives in 2014. Sony Pictures Studio was breached in 2014 when large amounts of confidential documents were stolen by cybercriminals who called themselves "Guardians of the Peace."[35] These cybercriminals then posted massive amounts of internal Sony documents in the weeks following the breach, many of which included embarrassing information

---

32. LIFELOCK, *supra* note 29. Target initially confirmed that 40 million customers' debit and credit card information was stolen. Then, weeks later, Target stated that 70 million people's email and mailing addresses were stolen.

33. Jethro Mullen & Seth Fiegerman, *Yahoo Tops the List of Largest Ever Data Breaches*, CNN BUS. (Oct. 4, 2017, 5:20 AM), https://money.cnn.com/2017/10/04/technology/yahoo-biggest-data-breaches-ever/index.html.

34. Soo Youn, *Marriott's Data Breach is Large, But It's Not the Largest: These are the Five Worse Corporate Hacks*, ABC NEWS (Nov. 30, 2018, 6:07 PM), https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391.

35. Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.6727c19f1378.

about Hollywood stars.[36] Less than a month after the breach, the FBI concluded that the North Korean government was behind the security incident.[37] Guardians of the Peace targeted Sony because of the potential release of its new movie *The Interview*, a comedy about a pair of American journalists sent to assassinate North Korean dictator Kim Jong Un.[38] Although the Sony breach did not expose a large amount of consumer personal information, it did highlight the dangers that data breaches pose to our country.[39] The Sony breach displayed how a foreign country can inflict significant harm on a U.S. business, the U.S. government, and its citizens by targeting a business with a data breach.[40]

Following the highly-publicized Sony breach, data breaches continued to rise[41] in the U.S., leading to the year

---

36. *Id. See also* JOSEPHINE WOLFF, YOU'LL SEE THIS MESSAGE WHEN IT IS TOO LATE, 166 (Sandra Braman ed., 2018) ("they [the Sony hackers] were looking to cause chaos—to publicly shame and torment SPE [Sony Pictures Entertainment] and its employees before as wide a global audience as possible by any means available, ranging from releasing high-level executives' embarrassing email exchanges and salary data, to posting employee Social Security numbers and financial information, to disseminating as-yet-unreleased movies and scripts.").

37. WOLFF, *supra* note 36, at 172. *See also* Jake Miller, *FBI Sources: Sony Pictures Cyberattack Traced to North Korea*, CBS NEWS (Dec. 18, 2014 7:52 PM), https://www.cbsnews.com/news/fbi-north-korean-hackers-behind-sony-pictures-cyberattack/.

38. Miller, *supra* note 37; *see also* Peterson, *supra* note 35 ("Sony Pictures canceled the theatrical release of the film Wednesday, responding to a vague threat against theaters showing the film supposedly posted by the hackers.").

39. Julia Boorstin, *The Sony Hack: One Year Later*, CNBC (Nov. 25, 2015, 10:26 AM), https://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html. ("The [Sony] hack revealed the personal information of tens of thousands of people, exposed embarrassing email exchanges between high-powered actors and executives").

40. See WOLFF, *supra* note 36, at 172–81.

41. *See* Charles Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN BUS. (Feb. 6, 2015, 10:52 AM), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (discussing the health insurer Anthem, Inc.'s breach in 2015, which affected 78.8 million customers, exposing names, addresses, Social Security numbers, and even employment information of current and former customers.). *See also* U.S. Office of Personnel Management,

2017 where data breaches reached an all-time high of 1,579 breaches in one year.[42] The most notable data breaches in 2017 were the Uber and Equifax data breaches, which dominated news headlines. The Equifax data breach affected over 140 million Americans and is discussed extensively in Part III of this Comment.[43] Outside of the Equifax data breach, the second most prominent data breach disclosed in 2017 was the Uber data breach. Although the security breach occurred in 2016, Uber executives concealed the breach from the public for over a year and finally publicly disclosed the breach in November 2017.[44] On November 21, 2017, Uber's CEO disclosed that 57 million users' personal information had been breached, which included some 600,000 names and driver's license numbers in the United States, as well as names, email addresses, and mobile phone numbers of riders.[45] A strong reaction followed the Uber data breach because of the way the company completely mishandled the security breach. Uber customers were shocked and outraged that a company would pay hackers to cover up a breach and allow the public to go uninformed that their personal information was in the hands of cybercriminals for over a

Cybersecurity Incidents, OPM.GOV, https://www.opm.gov/cybersecurity/cyber security-incidents/ (discussing the United States Personnel Management 2015 breach exposing personal information of 21.5 million current, former, and prospective federal employees).

42. CyberScout, *2017 Annual Data Breach Year-End Review*, IDENTITY THEFT RESOURCE CTR., 3 (2017), https://www.idtheftcenter.org/images/breach/2017 Breaches/2017AnnualDataBreachYearEndReview.pdf.

43. *See infra* Part III.

44. *See* Andy Greenberg, *Hack Brief: Uber Paid Off Hacker's to Hide a 57-Million User Data Breach*, WIRED (Nov. 21, 2017, 7:56 PM), https://www.wired .com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/ (stating that "Uber paid a $100,000 ransom to its hackers to keep the breach quiet and delete the data they'd stolen. It then failed to disclose the attack to the public—potentially violating breach disclosure laws in many of the states where its users reside—and also kept the data theft secret from the FTC.").

45. Dara Khosrowshahi, *2016 Data Security Incident*, UBER NEWSROOM (Nov. 21, 2017), https://www.uber.com/newsroom/2016-data-incident/.

year.[46] Although Uber acted in a completely unprofessional and unethical manner, the company's reaction to the breach underscores how important data security is to a company, as well as the strong incentive a company has to prevent a breach from occurring in the first place.[47] However, by failing to disclose the breach in hopes of dodging negative publicity, Uber violated multiple data breach notification laws. This led to Uber ultimately agreeing to pay $148 million in a joint settlement it reached with the top law enforcement officers in all fifty U.S. states.[48]

This past year has been a banner year for data breaches in the United States. Multiple retailers disclosed data breaches in 2018, most notably Macy's, Adidas, Best Buy, and Saks Fifth Avenue.[49] However, none of these retail breaches compare to the highly publicized breaches that occurred at Facebook, Marriott, and Under Armour in 2018. On March 29, 2018, Under Armour stated in a press release that a security issue occurred with MyFitnessPal, the company's food and nutrition application and website, in February 2018.[50] After an investigation, Under Armour

---

46. *See* Tom Ball, *Uber Data Breach Scandal: A Shocked Tech Industry Reacts to the Cover Up*, COMPUT. BUS. REV. (Nov. 22, 2017), https://www.cbronline.com/cybersecurity/breaches/uber-data-breach-scandal-cover-up-reaction/.

47. *See* PONEMON INST., 2018 COST OF A DATA BREACH STUDY 29 (2018) [hereinafter 2018 PONEMON INST. STUDY] (stating that "the cost of lost business was particularly high for US organizations ($4.20 million). This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill."). Therefore, Uber had a strong financial incentive to hide its data breach because of the damage a data breach does to a company's reputation. *See also infra* Section II.A.2.

48. Ben Kockman, *Uber, States Strike $148M Deal to End Data Breach Dispute*, LAW360: CYBERSECURITY & PRIVACY (Sept. 26, 2018), https://www.law360.com/cybersecurity-privacy/articles/1086585/uber-states-strike-148m-deal-to-end-data-breach-dispute.

49. Dennis Green & Mary Hanbury, *If You Shopped at These 16 Stores Last Year, Your Data Might Have Been Stolen*, BUS. INSIDER (Aug. 22, 2018, 5:39 PM), https://www.businessinsider.com/data-breaches-2018-4.

50. Under Armour, Inc., *Under Armour, Under Armour Notifies MyFitnessPal Users of Data Security Issue*, UNDER ARMOUR (Mar. 29, 2018, 4:30 PM),

found that 150 million user accounts were affected by the security breach.[51] The breach exposed users' usernames, email addresses, and passwords, but no payment information was breached.[52]

Then, on September 28, 2018, Facebook announced a data breach that exposed fifty million user accounts.[53] This breach gave hackers the ability to take over accounts, impersonating users and accessing private information about these people and their friends.[54] Although Facebook executives stated that there was no evidence that users' password or credit card information was exposed, this breach still gave hackers information that could be used for identity theft.[55] The most significant aspect of the Facebook data breach is the possibility for Facebook to be liable under the new European Law, the General Data Protection Regulation.[56] The Irish Data Protection Commission launched an investigation into Facebook shortly after the company announced the breach and the investigation "will examine Facebook's compliance with its obligation under the General Data Protection Regulation (GDPR) to implement

---

http://www.uabiz.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue.

51. *Id.*

52. Lisa Marie Segarra, *Under Armour Breach Exposes 150 Million MyFitnessPal Accounts*, TIME: SECURITY (Mar. 30, 2018), http://time.com/5222015/under-armour-myfitnesspal-data-breach/.

53. Allison Grande, *Facebook Breach Leaves 50M User Accounts Exposed*, LAW360 (Sept. 28, 2018, 9:48 PM), https://www.law360.com/articles/1087537?utm_source=ios-shared&utm_medium=ios&utm_campaign=ios-shared.

54. Deepa Seetharaman & Robert McMillan, *Facebook Finds Security Flaw Affecting Almost 50 Million Accounts*, WALL ST. J. (Sept. 28, 2018, 7:17 PM), https://www.wsj.com/articles/facebook-flaw-allowed-hackers-to-take-over-user-accounts-1538153947.

55. *Id.*

56. Sam Schechner, *Facebook Faces Potential $1.63 Billion Fine in Europe Over Data Breach*, WALL ST. J. (Sept. 30, 2018, 2:08 PM), https://www.wsj.com/articles/facebook-faces-potential-1-63-billion-fine-in-europe-over-data-breach-1538330906.

appropriate technical and organisational measures to ensure the security and safeguarding of the personal data it processes."[57] The investigation into Facebook's compliance with the GDPR is extremely significant because it is the first high-profile GDPR investigation and Facebook could ultimately face a $1.63 billion fine if found to be noncompliant with the law.[58]

Finally, 2018 ended with a massive data breach disclosure when Marriott announced on November 30, 2018, that hackers breached its Starwood reservation system and stole the personal data of 500 million guests.[59] The Marriott breach started back in 2014 and affected customers who made reservations for Marriott-owned hotel rooms from 2014 to 2018.[60] After further review, Marriott announced on January 4, 2019, that 383 million guests were affected by the breach, not the 500 million originally reported.[61] Marriott also revealed that the data breach exposed guests' passport numbers, email addresses, and payment card data.[62] The

57. Caroline Spezio, *GDPR Gets Early Test with Ireland's New Probe into Facebook's Big Breach*, CORP. COUNSEL (Oct. 3, 2018, 7:07 PM), https://www.law.com/corpcounsel/2018/10/03/gdpr-gets-early-test-with-irelands-new-probe-into-facebooks-big-breach/.

58. Schechner, *supra* note 56. ("Under GDPR, companies that don't do enough to safeguard their users' data risk a maximum fine of €20 million ($23 million), or 4% of a firm's global annual revenue for the prior year, whichever is higher. Facebook's maximum fine would be $1.63 billion using the larger calculation.").

59. Aisha Al-Muslim et al., *Marriott Says Starwood Data Breach Affects Up To 500 Million People*, WALL ST. J. (Nov. 30, 2018, 8:02 PM), https://www.wsj.com/articles/marriott-says-up-to-500-million-affected-by-starwood-breach-1543587121.

60. Nicole Perlroth et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

61. Connie Kim, *Marriott Provides Update on Starwood Database Security Incident*, MARRIOTT INT'L: NEWS CTR. (Jan. 4, 2019), http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/.

62. Kirsten Grind & Dustin Volz, *Marriott Says Hackers Swiped Millions of Passport Numbers*, WALL ST. J. (Jan. 4, 2019, 6:34 PM), https://www.wsj.com/articles/marriott-says-hackers-swiped-millions-of-passport-numbers-11546605000.

compromise of passport information is especially dangerous as it would be extremely valuable to foreign spies. Accordingly, the Federal Bureau of Investigation is leading an investigation into the Marriott hack to determine who was behind the hack.[63] Similar to Facebook, Marriott may also potentially be liable under the GDPR if it is found that Marriott was noncompliant.[64] In all, many high-profile data breaches occurred in 2018 and further emphasized the need for changes in the law to protect consumers and prevent data breaches in the future.

II. NEGATIVE EFFECTS ON THE AMERICAN ECONOMY

The increased frequency of data breaches in recent years has created large negative effects on the American economy and society in general. Data breaches cause problems for three distinct groups in America. Data breaches negatively affect (1) the organization that is breached, (2) the consumers that have had their personal information stolen, and (3) the economy as a whole.[65] This Part will discuss, exclusively, how security breaches negatively affect each of these three groups.

A. *The Effect on the Breached Organization*

First, data breaches are enormously costly for the organization that is breached. An organization that has experienced a data breach suffers a loss in two ways: (1) incurring increased expenses and (2) losing future revenues and profits through customer loss and damage to an

63. *Id.*

64. *See* Joyce Hanson, *Hospitality Cases and Trends to Watch in 2019*, LAW360 (Jan. 1, 2019), https://www.law360.com/articles/1110261/hospitality-cases-and-trends-to-watch-in-2019; *see also* Dan Clark, *Experts: Marriott's In-House Team Has Much Work Ahead*, CORP. COUNSEL (Dec. 3, 2018, 6:46 PM), https://www.law.com/corpcounsel/2018/12/03/experts-marriotts-in-house-team-has-much-work-ahead/.

65. *See infra* Sections II.A, B, C.

organization's reputation.[66]

1. Increased Expenses

A company subjected to a data breach will initially suffer loss from increased expenses due to increased legal fees and notification costs.[67] A study of the cost of data breaches is conducted each year by The Ponemon Institute.[68] These studies show that the United States consistently leads the world, by a significant margin, in data breach costs.[69] The Ponemon Institute's *2018 Cost of a Data Breach Study: Global Overview* found that the average cost of a data breach in the United States is $7.91 million, which is almost double the average global cost.[70] A large portion of these costs associated with data breaches are a result of increased legal fees and notification costs.[71] American companies that are breached spend $1.76 million of the $7.51 million total cost of a data breach on post data breach response activities.[72] These post data breach response activities include "help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory

66. *See* DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW, § 42.10 (Matthew Bender, rev. ed. 2019).

67. *See id.*

68. PONEMON INST., *Why We Are Unique* (2018), https://www.ponemon.org/about-ponemon. The Ponemon Institute is a research center dedicated to privacy, data protection, and information security policy that releases a yearly review of the cost of data breaches.

69. *See* 2018 PONEMON INST. STUDY, *supra* note 47, at 9.

70. *Id.* at 15. The global average cost of a data breach $3.86 million. The Middle East is the second costliest at an average cost of $5.31 million.

71. *Id.* at 6; *See also* BUS. INSIDER, *Data breaches cost US businesses an average of $7 million—here's the breakdown* (Apr. 27, 2017 11:00 AM), http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4 [hereinafter BUS. INSIDER] (Establishing legal costs as one of the ten biggest expenses of a data breach.).

72. *See* 2018 PONEMON INST. STUDY, *supra* note 47, at 9.

interventions."[73] Included as part of the post data breach response activities are notification activities which, once again, the United States leads the world in this data breach cost category.[74] The average American business spends $740,000 on notification costs per breach, which is $440,000 more than the second leading region for notification costs, the Middle East.[75] The United States' fragmented regulatory approach is the leading contributor to these notification costs[76] because the many different notification laws make compliance incredibly costly and burdensome for American businesses.[77]

Currently, there are fifty separate state data breach notification laws in the United States, all with different requirements for notification and differing levels of severity for noncompliance.[78] As one would imagine, the variation among state data breach notification laws makes compliance after a breach extremely complex and difficult.[79] When an

---

73. *Id.* at 28.

74. *See id.* at 9, 27. Although the Ponemon Institute considers post-breach data response and notification costs as two separate cost centers, both are part of the costs that occur post-breach and require compliance with the multitude of U.S. notification laws.

75. *See id.* at 5, 27. The Ponemon Institute studied the Middle East region as a whole, which for this study included the United Arab Emirates and Saudi Arabia.

76. *Id.* at 6. The Ponemon Institute provides examples of notification costs including: "Emails, letters, outbound telephone calls, or general notice that personal information was lost or stolen. Communication with regulators; determination of all regulatory requirements, engagement of outside experts [(i.e. attorneys)]."

77. *See* Herb Wisebaum, *The Total Cost of a Data Breach—Including Lost Business—Keeps Growing*, NBC NEWS (July 30, 2018, 3:15 PM), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826.

78. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [hereinafter NCSL] (providing a list of all fifty state data breach notification laws).

79. *See* BENDER, *supra* note 66, at § 42.04.

entity discovers that there has been a breach in its system one of the first action steps, among other things,[80] is to call a lawyer or team of lawyers to address the complexities of data breach notification laws.[81] These lawyers have the crucial task of identifying which state laws have been triggered by the breach and the requirements under each law.[82]

Once an organization experiences a data breach, it will have to navigate the many differing compliance requirements under the fifty different notification statutes. First, an organization will need to determine if it is required to notify state agencies in addition to notifying affected individuals. Some state laws have no state agency notification requirement at all.[83] Other state laws require notification to state agencies only if a certain number of residents of the state are affected by the breach, whereas other states require notification to state agencies regardless of the number of affected residents.[84] After determining whom to notify, an organization will need to determine if there is a specific time requirement within which it has to notify affected individuals. Some states require notification within a specific time frame, while others simply require

---

80. *Id.* ("Forensic experts may be needed to determine exactly which personal data was affected by the breach, public relations experts may be needed to draft and send letters to affected individuals, and management will need to meet and make decisions whether to go beyond what the law requires.").

81. *Id.*

82. *Id.*

83. *See* DIGITAL GUARDIAN, *The Definitive Guide to U.S. State Data Breach Laws* (2018) [hereinafter Definitive Guide to U.S. State Data Breach Laws].

84. *See id. See also* Maya Atrakchi et. al., *State Data Breach Notification Laws: Overview of the Patchwork*, JD SUPRA (Apr. 10, 2018), https://www.jdsupra.com/legalnews/state-data-breach-notification-laws-73889/; Jeffrey Kosseff, *My Company Has Had a Breach: Whom Do I Have to Notify?*, IAPP: THE PRIVACY ADVISOR (Mar. 21, 2016), https://iapp.org/news/a/my-company-has-had-a-breach-who-do-i-have-to-notify/. ("About 20 states require companies to notify state regulators if they have informed customers of a data breach, though some of these states only require regulator notice if a minimum number of individuals have been notified (typically 500 or 1,000).").

notification "without unreasonable delay."[85] The state statutes that do require a specific time frame all have varying time frames within which an organization must notify affected consumers.[86]

Then, after determining the various notification requirements and time frames, a corporation will need to determine what form the notices to individuals must take to ensure compliance with each statute. Some statutes require a direct notification to consumers with written mail or email, whereas other statutes simply allow posting a notice in a general circulation newspaper to satisfy notice.[87] Finally, after determining the form in which an individual must be notified, breached organizations must determine what information must be included in the notification to affected individuals. Some states require specific information to be included in the notice such as the date(s) of the breach, a description of the information accessed by hackers, a telephone number to call for further information, and a host of other information.[88] On the other hand, some state

85. *See* Definitive Guide to U.S. State Data Breach Laws, *supra* note 83. *See, e.g.*, IND. CODE § 4-1-11; ALASKA STAT. § 45.48.010 (2018); IOWA CODE ANN. § 715C.2 (West 2018); KAN. STAT. ANN. § 50-7a02 (West 2019); MASS. GEN. LAWS § 93H-3; MONT. CODE ANN. § 2-6-1503 (West 2019) (All of these state statutes simply require an organization that has been breached to notify consumers "without unreasonable delay" and provide little guidance as to what constitutes an unreasonable delay.).

86. *See, e.g.*, 2018 S.B. 318, Act. No. 396 (requiring notification within 45 days in Alabama); FLA STAT. ANN. § 501.171 (West 2019) (requiring notification within 30 days in Florida); S.D. COD. LAWS § 20-40-20 (requiring notification within 60 days in South Dakota).

87. *See, e.g.*, UTAH CODE § 13-44-101 (allowing notification by first-class mail, electronically, over the phone, or publication in a newspaper); S.B. 318, Act. No. 396 (requiring notification either by mail or email); CAL. CIV. CODE § 1798.82 (West 2019) (requiring notice to be either in written form or electronic format consistent with E-SIGN).

88. *See, e.g.*, HAW. REV. STAT. ANN. § 487N-2 (West 2019) (requiring the notice to contain clear and concise information regarding the type of covered information that was accessed or acquired, a general description of the incident, what actions a consumer should take to prevent their covered information from

statutes do not require any specific information to be included in the notification and let the breached organization decide what information it will provide.[89] In sum, fifty separate state notification breach statutes create an enormous compliance burden for a breached organization. Consequently, these compliance burdens have caused a significant increase in cost to a breached organization, which ultimately leads to the United States leading the world in data breach costs.

2. Lost Future Revenue and Profit

A data breach will have a substantial effect on customer loyalty, which causes organizations to lose future revenues and profits following a data breach. A 2017 study found that 70% of consumers would stop doing business with a company if it experienced a data breach.[90] In the United States specifically, consumers are much more likely to leave a company that has experienced a breach because they have more alternatives to turn to after a breach, thereby making their loyalty harder to preserve.[91] With more notification statutes passed into law in recent years and data breaches dominating the news headlines, American consumers are now more aware of data breaches and have higher

---

further access or misuse, and a telephone number that consumers can call for further information and assistance); FLA. STAT. ANN. § 501.171 (West 2019) (requiring notice to include at least: date(s) of the breach; a description of the covered information accessed or believed to be accessed; and contact information for the covered entity).

89. *See* ALASKA STAT. ANN. § 45.48.010 (West 2018); ARK. CODE ANN. § 4-110-105 (West 2018); DEL. CODE ANN. tit. 6, § 12B-101 (West 2018) et. seq.; 2018 S.B. 318, Act. No. 396 (All of these state notification statutes do not provide a requirement for specific information that must be included in the notification to consumers; it is left up to the breached organization to decide what information to include in the notification.).

90. *See* GEMALTO, Data Breaches and Customer Loyalty 2017. Gemalto is an international digital security company that conducted a study on the effects of a data breach on consumer loyalty in 2017.

91. 2018 PONEMON INST. STUDY, *supra* note 47, at 29.

expectations regarding how companies should help them following a breach.[92]

The increased consumer awareness has resulted in the United States leading the world in lost business following a security breach. Accordingly, a data breach costs American organizations an average of $4.2 million in lost business.[93] This cost component includes increased turnover of customers, greater customer acquisition activities, reputation losses, and diminished goodwill.[94]

The enormous cost of lost business has the negative consequence of incentivizing companies to hide a security breach from the public. The Uber and Equifax breaches are prime examples. When Equifax was breached in 2017, the company waited two months to disclose the breach.[95] Worse than Equifax, Uber hid its 2016 data breach for over a year by paying hackers to hide the data breach.[96] It is now clear why Uber paid the hackers to keep the security breach quiet. Uber feared losing millions of dollars from lost business after disclosing the data breach. With 70% of consumers likely to stop doing business with Uber after finding out about a data breach and Lyft being a suitable alternative ride-hailing app, Uber was likely to lose millions of customers after disclosing its data breach.[97] Therefore, the current security breach environment in America incentivizes organizations to hide their data breaches because of the high costs and lost customers that will result following the disclosure of the breach.

---

92. *Id.*

93. *Id.* The Middle East has the second largest customer loss costs with an average of $2.18 million. Therefore, the cost of lost business in the U.S. is double that of any country in the world.

94. *Id.*

95. *See infra* notes 141–46 and accompanying text.

96. *See supra* notes 43–45 and accompanying text.

97. *See* GEMALTO, *supra* note 87, at 1.

B. *The Effect on Consumers That Had Their Personal Information Breached*

The individual affected most by a data breach is the individual whose personal information was stolen and now is in the hands of cybercriminals. The most obvious reason is that consumers whose information is stolen are at significant risk of having their information used to make fraudulent charges to their accounts. Outside of this obvious negative consequence to consumers, there are two significant negative effects of a data breach on the individual whose personal information was stolen. First, the person who has been a victim of a breach may not even be aware that her personal information was stolen.[98] Second, even if an individual is aware that her personal information has been stolen, there is little she can do to obtain recourse.[99]

The United States' patchwork approach to data breach notification laws is a fundamental reason why many Americans are left unaware that their personal information has been stolen after a security breach. Although some Americans simply have not put forth the effort to check to see if their data has been breached,[100] the current notification landscape in the United States does not make it easy to determine whether one has been affected by a breach. The lack of a uniform notification statute in the United States makes the likelihood of one learning of the theft

98. *See* Blanco, *supra* note 12; *see also* Paul Roberts, *For U.S. Consumers: Ignorance of a Data Breach is Bliss*, DIGITAL GUARDIAN (Dec. 21, 2017), https://digitalguardian.com/blog/us-consumers-ignorance-data-breaches-bliss (stating that although "U.S. consumers are deeply concerned about the privacy and security of the data they share online, [they] often assume that massive data leaks and thefts have miraculously spared their personal information from exposure.").

99. See *infra* Section IV.A.3, for a discussion of the current circuit split in data breach class action suits. This circuit split means that consumers who have had their data breached do not know if they will be compensated for their lost time and money.

100. *See* Pesce, *supra* note 12.

dependent on where one lives.[101] All fifty separate data breach notification statutes in the U.S. differ significantly in what they require organizations to disclose to consumers, as well as the manner in which to notify consumers that have been breached. In 2017, only about twenty states had specific provisions about how consumers must be notified and what information must be contained in the message.[102] There are also varying levels of stringency within these twenty state data breach notification provisions.[103] For example, in Utah, simply posting in a general circulation newspaper is sufficient.[104] Conversely, in California, there are stricter data breach notification laws that require an entity to use a broader media notification and send an email message to all people who may be affected.[105]

Consequently, due to the ambiguity and variation among state data breach notification laws, many Americans are left unaware that their personal information is in the hands of cybercriminals.[106] A consumer that lives in a state with a weak notification law, such as Utah, may not be personally notified at all because the notification statute does not require personal notification.[107] Additionally, because of the enormous variation among the notification laws, it is easy for an organization to fail to comply with the requisite

---

101. Roberts, *supra* note 95.

102. Blanco, *supra* note 12.

103. *Id.*

104. UTAH CODE ANN. § 13-44-202(5)(iv)(A) (West 2009); *see also* Blanco, *supra* note 12.

105. CAL. CIV. CODE § 1798.29 (West 2017); Blanco, *supra* note 12. California law also requires that the notification must be written "in plain language" and provides the specific headings to incorporate in the notification.

106. *See* Blanco, *supra* note 12.

107. *See* UTAH CODE ANN. § 13-44-202(5)(iv)(A). *See, e.g.*, Blanco, *supra* note 12 (explaining that inconsistent state laws result in not all consumers having adequate protection in the event of a data breach and, in the case of Equifax, millions of consumers still had not been notified that they were affected by the breach three months after it occurred).

notification statute, thereby leaving consumers unaware that their personal information has been breached.[108]

Even if consumers are aware that their personal information has been breached, current U.S. law does not provide consumers with an avenue for the requisite recourse. When an individual discovers they have been a victim of a data breach, they must act immediately to protect their assets. These actions include: creating a fraud alert and monitoring accounts, obtaining copies of credit reports, as well as potentially placing a credit freeze on credit files and purchasing credit monitoring.[109]

These breached individuals spend valuable time and money protecting themselves from further harm.[110] Subsequently, these individuals should be able to recoup the lost time and money they were required to spend protecting their personal information and assets after the security breach. However, the current circuit split in the law does not always allow the affected consumers to sue as a class.[111] Presently, circuits are split over whether plaintiffs meet the standing requirements under Article III of the U.S. Constitution in data breach class action cases.[112] The Second,

---

108. *See supra* notes 78–86 and accompanying text.

109. *See* Susan Henson, *Here's What You Should Do After a Data Breach*, EXPERIAN (Sept. 8, 2017), https://www.experian.com/blogs/ask-experian/heres-what-you-should-do-after-a-data-breach/; *see also* Seena Gressin, *The Equifax Data Breach: What to Do*, F.T.C. (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

110. Experian credit monitoring costs $4.99 for the first month and then $24.99 for the months following. *Credit Monitoring*, EXPERIAN, https://www.experian.com/consumer-products/credit-monitoring.html (last visited Feb. 1, 2019) [hereinafter EXPERIAN CREDIT MONITORING]. *See* N. Gregory Mankiw, PRINCIPLES OF ECONOMICS, 5–6 (Jane Tufts et al. eds., 2018) ("The opportunity cost of an item is what you give up to get that item.").

111. *See infra* Part IV; *see also* Luke Martin, *Resolving the Circuit Split on Article III Standing for Data Breach Suits*, COLUM. BUS. L. REV. (Feb. 17, 2019 10:00 PM), https://cblr.columbia.edu/resolving-the-circuit-split-on-article-iii-standing-for-data-breach-suits/.

112. *See* Bradford, *supra* note 8, at 1327; *see also infra* Part IV.

Third, and Eighth Circuits have all recently held that plaintiffs in a data breach class action case lacked the appropriate standing under Article III of the Constitution. Conversely, the D.C., Sixth, Seventh, and Ninth Circuits have held that plaintiffs do meet the standing requirements under Article III.[113] This current split in the law makes it difficult for consumers to file a class action lawsuit and survive a motion to dismiss based on lack of standing. Therefore, those consumers that have had their personal information stolen in a data breach are left not knowing whether they will have any remedy for the harm they just suffered.

C. *The Effect on the Economy as a Whole*

Ultimately, these negative effects take a toll on the entire economy, and all American consumers are left suffering from the consequences of the many security breaches that occur every year. Although American organizations suffer a large increase in costs after a data breach, the majority of these costs are not ultimately paid for by the entity that was breached. Rather, these costs are passed on to the consumer.[114]

---

113. Jason C. Gavejian et al., *Fourth Circuit Weighs in on Standing in Data Breach Litigation*, NAT'L L. REV. (July 2, 2018), https://www.natlawreview.com/article/fourth-circuit-weighs-standing-data-breach-litigation ("Circuit courts have been split on the issue of standing in the data breach context, with some courts finding standing where only a heightened 'risk of future harm' exists, *i.e.* the likelihood that stolen data may be misused (Sixth, Seventh, and Ninth Circuits), while other circuit courts require actual harm such as financial loss (Second, Third, and Eighth Circuits).").

114. *See* Mankiw, *supra* note 110, at 499 (explaining the consumer price index ("CPI") and the produce price index ("PPI"), the author states "[b]ecause firms eventually pass on their costs to consumers in the form of higher consumer prices, changes in the PPI are often thought to be useful in predicting changes in the CPI."). *See generally*, MILTON FRIEDMAN, THERE'S NO SUCH THING AS A FREE LUNCH 95–96 (1975). In the context of corporate taxes, Milton Friedman explains that a corporation is "a pure intermediary through which its employees, shareholders, and stockholders cooperate for their mutual benefit." That is, the money sent to the IRS for taxes comes from the company's employees, customers,

As an example, the 2013 Target data breach resulted in financial institutions absorbing many of the costs and then passing these costs onto consumers.[115] Banks, credit unions, and credit card companies will then pass these costs onto consumers in the form of higher average interest rates and service fees to their customers.[116] Financial institutions are not alone, as all organizations will pass on the cost of a data breach to consumers. Retailers pass their increased expenses from a data breach onto their customers in the form of higher overall prices for goods and services.[117] Even if a company has insurance that covers the data breach, the consumer still pays these costs when the insurer ultimately increases its premium to the breached company and that company inevitably passes this increased cost onto its customers.[118]

An additional cost to the entire economy is the indirect cost of increased taxes paid to law enforcement. In 2017, the

---

and stockholders. This economic principle is called "there is no such thing as a free lunch," meaning that even if something is offered as "free" there is always a hidden indirect cost. The term originated from American saloons offering free lunches to patrons but requiring them to purchase drinks in order to get them. Therefore, the "free lunch" was paid for by the customer in the price of the drink. *See* TYLER COWEN, AN ECONOMIST GETS LUNCH, 63–67 (2012). Applying these economic principles to data breaches, we see that, ultimately, the consumer will bear the burden of paying the enormous costs of security breaches. When a company suffers a breach, it incurs increased costs associated with the breach. However, the company does not bear the burden of these costs; they are eventually passed on to the consumer through increased prices and fees.

115. *See* Ryan Tracy, *In a Cyber Breach, Who Pays, Banks or Retailers?*, WALL ST. J. (Jan. 12, 2014), https://www.wsj.com/articles/in-a-cyber-breach-who-pays-banks-or-retailers-1389572452 (stating that post-breach banks and credit unions carry the burden of closing accounts and reissuing new credit and debit cards).

116. Michael D. Simpson, Comment, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 683 (2016).

117. BUS. VIBES, *Data Breaches: How the Costs Gets Passed to Consumers* (Aug. 23, 2014), https://www.business2community.com/tech-gadgets/data-breaches-costs-gets-passed-consumers-0977859 [hereinafter BUSINESS VIBES].

118. *Id. See* Mankiw, *supra* note 110, at 499. *See also* Neil Amato, *The Hidden Costs of a Data Breach*, J. OF ACCOUNTANCY (July 25, 2016), https://www.journalofaccountancy.com/news/2016/jul/hidden-costs-of-data-breach-201614870.html.

FBI's Internet Crime Complaint Center received over 300,000 victim complaints.[119] American citizens pay for this law enforcement through taxes. Consequently, more security breaches will, in turn, mean more tax dollars put into law enforcement's efforts to combat fraud and cybercriminals.[120] This ultimately results in increased strain on taxpayers and the entire U.S. economy due to the increasingly large number of security breaches.

Data breaches also have a negative effect on the job market.[121] A 2013 study by the Center for Strategic and International Studies postulated that cybercrime cost the U.S. economy 500,000 jobs lost in 2013.[122] Although this is not the net loss as many workers will find other jobs, cybercrime and data breaches may cause underemployment if displaced workers do not find jobs that pay as well.[123] Indeed, as the number of data breaches has increased significantly since 2013, the cost to the economy has also risen.[124] The Center for Strategic and International Studies

---

119. Sam Wood, *FBI Reports Cybercrime Cost the U.S. $1.4B in 2017, but the Actual Number is Probably Even Bigger*, GOV'T TECH. (May 10, 2018), http://www.govtech.com/security/FBI-Reports-Cybercrime-Cost-the-US-14B-in-2017-but-the-Actual-Number-is-Probably-Even-Bigger.html (stating that the "second most reported offense was personal data breaches, which are used for identity theft or industrial espionage.").

120. *See* BUS. VIBES, *supra* note 117 ("indirect losses come in the form of higher taxes paid for increased law enforcement vigilance of fraud and regulatory compliance across the board.").

121. *Id.* (It is "estimated that the economy as a whole suffers a net loss of some 500,000 jobs per year due to fraud related expenses to companies."). *See also* Eamon Javers, *Cybercrime May Cost U.S. Economy $100 Billion, Says New Study*, CNBC (July 22, 2013), https://www.cnbc.com/id/100904224 ("cybercrime creates a $100 billion annual loss to the U.S. economy.").

122. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, The Economic Impact of Cybercrime and Cyber Espionage (2013) https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

123. *Id.*

124. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, The Economic Impact of Cybercrime—No Slowing Down (2018) https://www.mcafee.com/enter

2018 follow-up study found that cybercrime may cost the global economy $600 billion, or 0.8% of the global GDP.[125] The internet economy, the fastest growing segment of the global economy, was worth $4.2 trillion of the global economy in 2016.[126] Comparing the global internet economy to cybercrime, we can see that cybercrime is essentially a 14% tax on growth.[127] Taking all of these factors into account, it is clear that in the end, the entire American economy and its consumers bear most of the burden of paying the cost of security breaches.

In summary, data breaches have negative consequences on the organization that was breached, the individuals whose personal information was stolen, and the economy as a whole. There are multiple ways the American legal system could improve to help alleviate these negative consequences.[128] The infamous 2017 Equifax data breach incorporated all three of these negative consequences. Therefore, the Equifax data breach provides a great opportunity for the American legal system to help relieve the negative consequences of data breaches.

III. THE EQUIFAX DATA BREACH

On September 7, 2017, Equifax announced that criminal hackers attacked and infiltrated its servers.[129] This data breach affected approximately 143 million U.S. consumers, which accounts for nearly 44% of the U.S. population.[130] The

---

prise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

125. *Id.* at 4 (providing reasons for the increase in cybercrime's cost to the global economy).

126. *Id.* at 19.

127. *Id.* ("There would be real benefit to development and prosperity in all countries if the international community made a concerted effort to reduce [cybercrime].").

128. *See infra* Part V.

129. EQUIFAX, *supra* note 2.

130. *See id.*

information accessed included "names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers."[131] In February of 2018, nearly five months after Equifax disclosed the breach, the Wall Street Journal reported that the breach was even worse than first imagined and the stolen data also included tax identification numbers, as well as driver's license states and issuance dates.[132] Needless to say, Equifax's data breach left millions of Americans vulnerable to identity theft.

The Equifax data breach is unlike any of the previous data breaches that American citizens have experienced.[133] Typically, data breaches involve a hacker stealing usernames and passwords for a specific account.[134] A hacker can use that information to access the user's account and set up more fake accounts under the user's name.[135] Hackers can also try to take advantage of the fact that many people use the same username and password by trying to use the same information to access accounts at other institutions. However, the Equifax data breach has the potential to be more damaging to consumers. This is because the information from the Equifax breach can bring context to the massive amount of data that has been stolen in recent years.[136] A cybercriminal can determine if a person has a legitimate account with a financial institution from the information received in the Equifax breach and combine that

131. *Id.*

132. AnnaMaria Andriotis, *Equifax May Be Worse Than You Think*, WALL ST. J. (Feb. 9, 2018), https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370.

133. Ricardo Villadiego, *The Equifax Data: Now That They Have It, How Will Hackers Use It?*, FORBES (Nov. 29, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/11/29/the-equifax-data-now-that-they-have-it-how-will-hackers-use-it/#2e6b56cb602c.

134. *Id.*

135. *Id.*

136. *Id.*

information with the username and password information from previous data breaches. This will allow cybercriminals to maximize account takeover and conversion to fraud for known accounts that contain significant amounts of money.[137] Outside of this unique attack, cybercriminals can also revert to the more traditional path of identity theft by opening fraudulent accounts using the victim's personal information.[138] Equifax's "breach exposed more than enough information about each [consumer] to apply for loans, credit cards, and checking accounts."[139] "Cybercriminals can use these funds outright, or they can physically move money from one account to another to 'cash out'" and obtain the actual funds these accounts are worth.[140]

To make matters worse, Equifax waited over a month to notify consumers about the data breach.[141] Equifax discovered the data breach on July 29, 2017.[142] However, the company did not publicly disclose the data breach until September 7, 2017.[143] This failure to notify consumers put these consumers in danger because their personal information could have been used to open fraudulent accounts, credit cards, apply for loans, and other actions that negatively affect consumers' finances. By failing to disclose the data breach for over a month, consumers were not able to take the appropriate preventative measures to protect their financial information such as credit monitoring and

---

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. Michael Hiltzik, *Here are all the ways the Equifax data breach is worse than you can imagine*, L.A. TIMES (Sept. 8, 2017), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html.

142. *Id.*

143. Elizabeth Weise, *A timeline of events surrounding the Equifax data breach*, USA TODAY (Sept. 26, 2017), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/.

setting up a credit freeze with all three credit bureaus.[144] Even after Equifax's public announcement of the data breach, millions of consumers are still unaware of the data breach.[145] As of November 2017, 71 million U.S. adults have not heard anything about the Equifax data breach.[146] As a result, millions of Americans are left in the dark, completely unaware that their personal information has been stolen and is potentially being used to harm them financially.

Failing to publicly disclose the data breach also allowed for potential insider trading within Equifax. Three of Equifax's top executives sold nearly $1.8 million of Equifax stock in August, which was after Equifax was notified of the data breach but prior to its public announcement of the breach.[147] When the data breach was made public on September 7, shares of Equifax dropped around 34.5%, falling from $142.72 to $92.98 per share.[148] Needless to say, these three top executives would not have made nearly as much money if they had sold their shares after the public announcement of the breach rather than before the announcement. This prompted the U.S. Justice Department to investigate whether these three top Equifax officials violated insider trading laws.[149] Equifax's board of directors also formed a special committee to investigate whether the three top officials that sold stock in August violated insider

144. *See* Gressin, *supra* note 109. *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#second.

145. Blanco, *supra* note 12.

146. *Id.*

147. Kevin McCoy, *Feds reportedly investigate Equifax executives' stock sales*, USA TODAY (Sept. 18, 2017), https://www.usatoday.com/story/money/2017/09/18/feds-reportedly-investigate-equifax-executives-stock-sales/677003001/.

148. *Id.*

149. Elena Holodny, *The Justice Department has reportedly opened an insider-trading investigation at Equifax*, BUS. INSIDER (Sept. 18, 2017), http://www.businessinsider.com/equifax-hack-justice-department-investigation-of-alleged-insider-trading-2017-9.

trading laws.[150] The committee concluded that none of the officials that sold stock engaged in insider trading because none of the executives had knowledge of the data breach when their trades were made.[151] Accordingly, this situation highlights another potential problem with failing to notify the public of a data breach; it creates a much larger potential for insider trading with public companies that are breached. The Equifax example illustrates the need for companies to disclose data breaches as soon as possible so that not only are consumers able to protect themselves, but it also does not allow for illegal insider trading activity within the company.

Finally, in late 2018, the United States House Oversight and Government Reform Committee released a report on its findings from a fourteen-month investigation into the 2017 Equifax data breach.[152] The report found two main points of failure by Equifax.[153] First, Equifax's management structure lacked accountability and had no clear lines of authority.[154] This poor structure led to a breakdown in communication between the company's IT policy development and its operations.[155] Equifax's second point of failure stemmed from its aggressive growth strategy and accumulation of data, which resulted in a complex IT environment.[156] This growth

150. Elena Holodny, *Equifax says its executives didn't engage in insider trading*, BUS. INSIDER (Nov. 3, 2017), http://www.businessinsider.com/equifax-hack-special-committee-says-no-insider-trading-2017-11.

151. *Id.*

152. U.S. H. R. COMM. ON OVERSIGHT AND GOV'T REFORM, 115TH CONG., THE EQUIFAX DATA BREACH (2018).

153. *Id.* at 4.

154. *Id.* at 4 ("[A] lack of accountability and no clear lines of authority in Equifax's IT management structure existed, leading to an execution gap between IT policy development and operation. This also restricted the company's implementation of other security initiatives in a comprehensive and timely manner. As an example, Equifax had allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains.").

155. *Id.* at 60–71.

156. *Id.* at 4 ("Equifax's aggressive growth strategy and accumulation of data

strategy resulted in Equifax maintaining credit information on 820 million customers and more than 91 million businesses in 2017.[157] With a massive amount of personal information in its system, Equifax was a prime target for hackers and its complex IT environment left Equifax unable to prevent an attack by hackers.[158] Accordingly, the report found that Equifax failed to implement an adequate security program to protect the massive amount of sensitive data Equifax held.[159] As a result, the report ultimately concluded that the Equifax data breach was entirely preventable.[160] The House Oversight Report further concluded that Equifax was unprepared to identify, alert, and support affected consumers after the breach.[161] In all, the House Oversight report was damning for Equifax and underscored its many shortcomings regarding the 2017 security breach.

The United States House Oversight and Government Reform Committee Report released in December 2018 reinforced the need for improvement in cybersecurity efforts in 2019 and beyond.[162] Additionally, the events following the

---

resulted in a complex IT environment. Equifax ran a number of its most critical IT applications on custom-built legacy systems. Both the complexity and antiquated nature of Equifax's IT systems made IT security especially challenging. Equifax recognized the inherent security risks of operating legacy IT systems because Equifax had begun a legacy infrastructure modernization effort. This effort, however, came too late to prevent the breach.").

157. *Id.* at 15.

158. *Id.* at 18.

159. *Id.* at 2.

160. *Id.* ("Equifax, however, failed to implement an adequate security program to protect this sensitive data. As a result, Equifax allowed one of the largest data breaches in U.S. history. Such a breach was entirely preventable.").

161. *Id.* at 3 ("When Equifax informed the public of the breach on September 7, the company was unprepared to support the large number of affected consumers. The dedicated breach website and call centers were immediately overwhelmed, and consumers were not able to obtain timely information about whether they were affected and how they could obtain identity protection services.").

162. *See id.* at 94–96 (providing recommendations to prevent data breaches and improve cybersecurity).

Equifax data breach highlighted the negative effects of a data breach. The current United States legal framework does not provide any help in alleviating these negative effects of a data breach. Therefore, the Equifax data breach provides a perfect opportunity for the U.S. legal system to adjust and improve consumer protection and cybersecurity efforts in America.

IV. ARTICLE III STANDING IN DATA BREACH CLASS ACTIONS AND THE CURRENT PRIVACY LAW LANDSCAPE

Currently, there are two areas of unsettled law significantly affecting companies and individuals involved in data breaches. These two areas of the law are: (1) the current circuit split regarding Article III standing in data breach class action cases and (2) the current privacy law landscape in the United States and abroad. First, this Part discusses the current circuit split and explains why courts grapple over whether consumers' increased risk of future harm satisfies the Constitution's Article III standing requirements. Then, this Part discusses the current privacy law landscape, specifically, two new laws implemented in the past year and how they affect organizations and consumers.

A. *Article III Standing*

To litigate in federal courts, plaintiffs must meet the Article III standing requirements in the United States Constitution.[163] Article III of the U.S. Constitution limits the authority of the federal judges to deciding "cases" and "controversies."[164] Article III's case and controversy requirement preserves the separation of powers within the three branches of government by preventing the unelected judiciary from exercising executive or legislative powers.[165]

---

163. *See* U.S. CONST. art. III., § 2.

164. *Id.*

165. *See* 13A CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE §

The Supreme Court requires three factors to be met to establish Article III standing: (1) "the plaintiff must have suffered an 'injury in fact'—an invasion of a legally protected interest[,] which is (a) concrete and particularized . . . and (b) 'actual or imminent, not "conjectural" or "hypothetical"'"; (2) "there must be a causal connection between the injury and the conduct complained of," meaning "the injury has to be 'fairly trace[able] to the challenged action of the defendant'"; and (3) "it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[166] This three-part test requires a plaintiff to establish Article III standing to satisfy the case-or-controversy requirement and thereby preserve the delicate balance of separation of powers.[167]

Following the 2017 data breach, hundreds of class action cases were filed against Equifax in federal and state court.[168] In data breach class action cases, such as the cases Equifax faces, plaintiffs allege that the defendant used inadequate security to protect the plaintiffs' personal data from being hacked.[169] In most cases, the plaintiff cannot prove that a hacker has used or sold the data to the plaintiff's detriment.[170] Accordingly, the plaintiff alleges that the defendant's failure to protect his personal data has caused him damage by increasing the risk of future harm from identity theft and imposed costs on the plaintiff when he

---

3531.3 (3d ed. 2017); Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 U. PA. L. REV. 1373, 1375 (2014).

166. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

167. REDISH & JOSHI, *supra* note 165, at 1375.

168. *Equifax Inc: Still Defends Suits Over 2017 Data Breach,* CLASS ACTION REPORTER (Jan. 2, 2019); *see generally*, Fed. R. Civ. P. 23 (setting forth rules for certifying class actions in federal courts).

169. MANK, *supra* note 8, at 1325. *See also* 3 IAN C. BALLON, E-COMMERCE & INTERNET LAW § 27.07 (Dec. 2017 Update).

170. MANK, *supra* note 8, at 1325.

takes measures to prevent future third-party data access.[171] Accordingly, the Equifax class action cases will inevitably turn on an analysis of whether the plaintiff's increased risk of future harm satisfies the "injury-in-fact" element of Article III standing.[172] As such, federal courts will have to decide whether the victims of the Equifax data breach had an "injury-in-fact" that was "actual or imminent" as well as "concrete or particularized."

Two recent court cases, *Clapper v. Amnesty International* and *Spokeo, Inc. v. Robins*, have shaped the current legal landscape in determining Article III standing in data breach cases.[173] The current circuit split surrounding the Article III standing requirements stems from various circuit courts' interpretation of these two cases. In *Clapper*, the Supreme Court analyzed the "actual or imminent" requirement of injury-in-fact for a data breach case,[174] whereas *Spokeo* analyzed whether a data breach case met the "concrete or particularized" requirement for injury-in-fact.[175]

---

171. Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 399–400 (2014) (discussing cases where "plaintiffs' information has been accessed but that information has not been used to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiffs. However, these plaintiffs typically claim that they have been harmed in other ways: incurring costs for credit-monitoring services, paying the costs of cancelling and receiving new bank cards, suffering loss of reward points from cancelled cards, and enduring general anxiety that their information will be used in the future to make unauthorized purchases." (footnote omitted)).

172. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, (D.D.C. 2014).

173. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 398 (2013).

174. *Clapper*, 568 U.S. at 398.

175. *Spokeo*, 136 S. Ct. 1540 at 1545.

1. Clapper: Injury must be "actual or imminent" for standing

The Supreme Court analyzed the "actual or imminent" requirement for Article III standing in a data breach case in *Clapper v. Amnesty Int'l USA*.[176] *Clapper* originates from the Foreign Intelligence Surveillance Act of 1978 (FISA), which "allows the Attorney General and Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States."[177] In 2008, the FISA Amendments Act (50 U.S.C. § 1881a) made two key changes to FISA that expanded the government's power to authorize foreign intelligence surveillance.[178] The *Clapper* plaintiffs are attorneys and human rights, labor, legal, and media organizations, who claim that they engage in sensitive international communications with individuals who they believe are likely targets of § 1881a surveillance.[179] These plaintiffs subsequently sued on the day the FISA amendments were enacted, seeking a declaration that the § 1881a is unconstitutional.

The *Clapper* case turns on whether plaintiffs suffered an injury-in-fact and therefore have established Article III standing.[180] Plaintiffs claim that they have established an injury-in-fact because "there is an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted under § 1881a at some point in

176. *Clapper*, 568 U.S. at 409.

177. *Id.* at 401.

178. *Id.* at 404 (First, "§ 1881a does not require the [g]overnment to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power." Second, it "does not require the government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.").

179. *Id.* at 406.

180. *See id.* at 407.

the future."[181] Justice Alito in his opinion for the Supreme Court rejected this argument.[182] The Court explained that the plaintiffs' argument for standing rests on a highly speculative fear that relies on "a highly attenuated chain of possibilities" and therefore does not satisfy the requirement that threatened injury must be certainly pending.[183]

Justices Breyer, Ginsburg, Sotomayor, and Kagan dissented.[184] In writing for the dissent, Justice Breyer stated that the harm the plaintiffs claim is not speculative.[185] Justice Breyer goes on to explain that based upon the record and "commonsense inferences," there is a very strong likelihood that the government will intercept at least some of the communications plaintiffs engage in while acting under the authority of § 1881a.[186] Justice Breyer gives four strong reasons why the government will intercept some of the communications in the future.[187] Therefore, the dissent concludes that there is a "high probability" that the government will intercept plaintiffs' communications and the plaintiffs' future harm is not at all speculative.[188]

---

181. *Id.* at 410.

182. *Id.*

183. *Id.*; *see also* Summers v. Earth Island Inst., 555 U.S. 488, 499 (2009) (rejecting a standing theory based on a speculative chain of possibilities); Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (reiterating that threatened injury must be certainly impending to constitute an injury-in-fact).

184. *Clapper*, 586 U.S. at 422 (Breyer, J., dissenting).

185. *Id.*

186. *Id.* at 427.

187. *Id.* at 427–29. First, the plaintiffs continue to engage in communication that § 1881a authorizes the government to intercept. Second, plaintiffs have a strong motive to engage in these conversations and the government has a strong motive to listen in on these conversations. Third, the government's past behavior indicates that it will continue to seek information about alleged terrorists and detainees "through means that include surveillance of electronic communications." "Fourth, the [g]overnment has the *capacity* to conduct surveillance of the kind at issue here."

188. *Id.* at 430–31.

Addressing the majority's reasoning that plaintiffs have failed to show that injury is certainly impending, the dissent argues that certainty is not and has never been the "touchstone of standing."[189] The dissent explains that the future is uncertain and all that is needed to support standing is that future injury is reasonably likely.[190] Therefore, Justice Breyer concludes his dissent by stating that the word "certainly" in "certainly impending" does not mean absolute certainty. Rather, the Constitution requires something more akin to reasonable probability or high probability to establish an injury-in-fact.[191]

In footnote 5 of the opinion, the majority acknowledged that an allegation of future injury *can* satisfy the immanency requirement if the threatened injury is "certainly impending," or there is a "substantial risk" that harm will occur.[192] However, the majority ultimately held that plaintiffs did not establish that injury is certainly impending or that there was a substantial risk that harm will occur because plaintiffs relied only on a speculative chain of possibilities for injury to occur.[193] Therefore, in a close 5-4 decision, the Supreme Court held that Plaintiffs lacked "Article III standing because they cannot demonstrate that the future injury that they purportedly fear is certainly impending."[194] The result of *Clapper's* close 5-4 decision, along with the "substantial risk" theory in footnote 5 and Justice Breyer's strong dissent, has led to some lower courts applying the alternative substantial risk standard for Article

189. *Id.* at 431.

190. *Id.*

191. *Id.* at 441.

192. *Id.* at 414, n.5 (majority opinion). *See also*, Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 141 (2010); Pennell v. City of San Jose, 485 U.S. 1, 8 (1988).

193. *Clapper*, 568 U.S. at 414.

194. *Id.* at 422.

III standing.[195]

2. *Spokeo*: Injury Must be "Concrete and Particularized" for Article III Standing

The Supreme Court recently explained the concrete and particularized standard to establish an injury-in-fact for Article III standing in *Spokeo Inc. v. Robins*.[196] This case arose from the search engine Spokeo conducting a search on plaintiff Robins' name and the website gathered and disseminated inaccurate information about the plaintiff.[197] After Robins discovered that inaccurate information about him was distributed, he filed a lawsuit on behalf of himself and a class of similarly situated people.[198] Robins alleged that Spokeo willfully failed to comply with Section 1681e(b) of the Fair Credit Reporting Act (FCRA), which requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy of consumer reports."[199]

The Ninth Circuit held that defendant's violation of the FCRA was sufficient to satisfy the injury-in-fact requirement for Article III standing, even though the plaintiff failed to allege any specific damages.[200] The Supreme Court then granted a writ of certiorari and analyzed the "concrete and particularized" requirement for an injury-in-fact to satisfy

195. *See In re* Zappos, Inc., 2018 WL 1883212 (9th Cir. 2018) (holding that plaintiffs established that there is a "substantial risk that harm will occur" to satisfy Article III standing); Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193, 200 (4th Cir. 2017) (discussing the substantial risk test from *Clapper* and ultimately holding that injury was too speculative to establish standing); Hedges v. Obama, 724 F.3d 170, 196, 201–03 (2d Cir. 2013) (discussing and applying the substantial risk test for pre-enforcement review of criminal charges under Section 1021 of the National Defense Authorization Act for Fiscal Year 2012).

196. Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016).

197. *Id.*

198. *Id.*

199. 15 U.S.C. § 1681e(b) (2010).

200. Robins v. Spokeo, Inc., 742 F.3d 409, 413 (9th Cir. 2014).

the first element of Article III standing.[201] The Court explained that for an injury to be particularized an individual must have been injured in a "personal and individual way."[202] Injury-in-fact must also be concrete.[203] However, the Ninth Circuit did not analyze the concreteness requirement. Rather, the Ninth Circuit held that Robins alleges concrete de facto injuries because he alleges a violation of his own statutory rights, meaning his personal interests in the handling of his credit information is individualized rather than collective.[204] Writing for the Supreme Court, Justice Alito rejected the Ninth Circuit's explanation. Justice Alito explained that Robins' alleged concrete de facto injuries concern only whether the injury is particularized and not whether it is concrete.[205] An injury must be real, not abstract, for it to satisfy the concreteness requirement for Article III standing.[206] The majority opinion in *Spokeo* did not define what exactly constitutes a concrete injury. However, citing *Clapper*, the Court did acknowledge that the "risk of real harm" can satisfy the concreteness requirement.[207] The Court explained that a tort claim can exist even if it is difficult to measure or prove.[208] Even with the risk of real harm analysis, the Supreme Court was not moved to hold that Robins had satisfied the concreteness requirement.[209]

---

201. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546 (2016).

202. *Id.* at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, n.1 (2016)).

203. *Id.*

204. *Id.*

205. *Id.*

206. *Id.*

207. *Id.* at 1549.

208. *Id.* (citing RESTATEMENT (SECOND) OF TORTS §§ 569, 570 (AM. LAW INS. 1979), which states that slander per se and libel can be established without special harm).

209. *See id.* at 1550.

Ultimately, the Supreme Court held that the Ninth Circuit's analysis regarding standing in *Spokeo* was incomplete because it failed to address the question of whether Robins' injury met the concreteness requirement for Article III standing.[210] Accordingly, the Supreme Court vacated the Ninth Circuit's judgment and remanded the case for further proceedings.[211] As a result, the Supreme Court's failure to provide specific guidance on the concreteness requirement in *Spokeo* has left lower courts and attorneys struggling to understand what constitutes a concrete injury.[212] Ultimately, the *Spokeo* decision leaves open the question of whether a data breach without financial losses and only increased risk of future harm can constitute a concrete injury for Article III standing.[213]

3. Circuit Split: Standing in a Data Breach Case

Following the Supreme Court's rulings in *Clapper* and *Spokeo*, circuit courts have been split on the issue of standing in a data breach case. Multiple courts have held that exposure of consumer data that elevates the risk of identity theft is sufficient to establish Article III standing.[214] Other circuits have held that elevated risk of identity theft is

---

210. *Id.*

211. *Id.*

212. *See* Amy Howe, *Opinion analysis: Case on standing and concrete harm returns to the Ninth Circuit, at least for now*, SCOTUSBLOG (May 16, 2016, 6:45 PM), http://www.scotusblog.com/2016/05/opinion-analysis-case-on-standing-and-concrete-harm-returns-to-the-ninth-circuit-at-least-for-now/. The author discusses how Spokeo, its supporters, and its lawyers were hoping for a "bright-line" rule, but instead were given a broader ruling in their favor. However, this may lead to a more definitive answer on this issue in the near future from the Supreme Court.

213. Mank, *supra* note 8, at 1356.

214. *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018); *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018); Attias v. CareFirst Inc., 865 F.3d 620, 623 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC 794 F.3d 688, 690 (7th Cir. 2015).

insufficient to establish standing.[215] The majority of these cases hinge on whether the injury is "actual or imminent" and "concrete or particularized" to satisfy the injury-in-fact requirement for Article III standing.

a. Circuit Courts Holding No Standing for Increased Risk of Future Harm

i. Second Circuit: *Whalen v. Michael Stores, Inc.*

In *Whalen v. Michael Stores, Inc.*, the Second Circuit held that Plaintiff Mary Jane Whalen did not satisfy Article III standing because she did not allege a particularized and concrete injury.[216] Ms. Whalen's personal information was stolen in the Michaels Stores, Inc. 2014 data breach.[217] Although Ms. Whalen's credit card information was used to make fraudulent purchases, she subsequently canceled her card and was not liable for her fraudulent purchases.[218]

Ms. Whalen claimed, inter alia, that she faces a risk of future identity fraud.[219] However, the Second Circuit rejected Ms. Whalen's claims because she did not suffer a "particular and concrete injury" to satisfy the constitutional standing requirements under Article III.[220] Ms. Whalen did not offer how she could plausibly face a threat of future fraud because her stolen credit card was promptly canceled after the breach and no other personal information was stolen in the breach.[221] Therefore, following the Supreme Court's

215. *See* Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc., 892 F.3d 613 (4th Cir. 2018); Alleruzzo v. SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017); Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017);

216. *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).

217. *Id.* at 90.

218. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

ruling in *Clapper*, the Second Circuit explained that Ms. Whalen did not allege a future injury that is "certainly impending" to establish Article III standing.[222] Accordingly, the Second Circuit held that Ms. Whalen did not suffer an injury-in-fact to satisfy the constitutional standing requirements and her claims were dismissed.[223]

ii. Eighth Circuit: *Alleruzzo v. SuperValu, Inc.*

In this case, defendants operated a chain of retail grocery stores that suffered two separate cybersecurity breaches, which exposed customer credit and debit card information.[224] Subsequently, plaintiffs sued as a class and argued that they sufficiently alleged an injury-in-fact because the theft of their card information created a substantial risk that they would suffer identity theft in the future.[225]

Plaintiffs relied on a 2007 Government Accountability Office (GAO) report to support their claim that the breach created a substantial risk of future harm.[226] However, the Eighth Circuit found that this report actually did not support their claim.[227] The Court stated that the GAO report concluded that compromised credit and debit card information could not be used alone to open new unauthorized accounts.[228] Additionally, the report found that most of the data breaches from 2000 to 2005 have not resulted in detected incidents of identity theft.[229] In light of this information, combined with the Supreme Court's ruling in *Clapper*, the Eighth Circuit concluded that plaintiffs are

222. *Id.* (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)).

223. *Id.*

224. *See* Alleruzzo v. SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).

225. *Id.* at 768.

226. *Id.* at 771.

227. *Id.*

228. *Id.* (quoting U.S. Gov't Accountability Off., GAO-07-737).

229. *Id.*

not at substantial risk of identity theft and plaintiffs' allegations of future injury do not support standing in this case.[230]

iii. Fourth Circuit: *Beck v. McDonald* & *Hutton v. National Board of Examiners in Optometry, Inc.*

Beck v. McDonald

This 2017 Fourth Circuit case stems from a laptop connected to a pulmonary functioning testing device that was stolen from a Veterans Affairs hospital.[231] This laptop contained encrypted personal information of approximately 7,400 patients.[232] A class action case was subsequently filed and plaintiffs sought to establish Article III standing based on the increased risk of future identity theft and the cost of measures to protect against it.[233]

The Fourth Circuit acknowledged that the threat of future injury can satisfy Article III standing requirements.[234] However, the Court held that the threat faced by the plaintiffs here was too speculative to establish standing.[235] The Fourth Circuit explained that, absent factual evidence, the assumption that the thieves stole the laptop and that the named plaintiffs would have their personal information stolen is much too speculative to establish standing.[236] Additionally, citing footnote 5 in

230. *See id.* at 771–72 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) ("[A]llegations of possible future injury are not sufficient.")).

231. Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).

232. *Id.* at 267. The information in the stolen laptop included birth dates, the last four digits of social security numbers, and physical descriptions of patients.

233. *Id.* at 266–67.

234. *Id.* at 271 (citing Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000)).

235. *Id.* at 274–75.

236. *Id.* at 274 ("[E]ven after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that

Clapper, the Fourth Circuit held that, in this case, standing cannot be established from the "substantial risk" that the harm from identity theft will occur.[237] The Court rejected Plaintiffs' argument that because, overall, 33% of health-related data breaches result in identity theft, they are at a substantial risk of harm to establish standing.[238] Finally, the Court also rejected Plaintiffs' claim that the future mitigation costs to guard against identity theft do not establish standing.[239] Therefore, following the ruling in *Clapper*, the Fourth Circuit affirmed the district court's ruling to dismiss the case for lack of standing under Article III.[240]

Hutton v. National Board of Examiners in Optometry, Inc.

In June of 2018, the Fourth Circuit held that Plaintiffs' established standing in a data breach case, but not on the basis of increased risk of future harm.[241] In *Hutton*, a class comprised of optometrists sued the National Board of Examiners in Optometry (NBEO) for injuries resulting from a data breach at NBEO.[242] The district court, citing *Beck*,

matter, that the thief stole the laptop with the intent to steal their private information.").

237. *Id.* at 275.

238. *Id.* at 275–76 ("Even if we credit the Plaintiffs' allegation that 33% of those affected by Dorn VAMC data breaches will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm.") (citing Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) stating 'general allegations . . . that data breach victims are 9.5 times more likely to suffer identity theft and that 19 percent of data breach victims become victims of identity theft' insufficient to establish 'substantial risk' of harm.").

239. *Id.* at 276–77 ("Simply put, these self-imposed harms cannot confer standing.") (citing Remijas v. Neiman Marcus Grp., LLC 794 F.3d 688, 694 (7th Cir. 2015) "Mitigation expenses do not qualify as actual injuries where the harm is not imminent.").

240. *Id.* at 278.

241. *See* Hutton v. Nat'l Bd. of Examiners in Optometry, Inc. 892 F.3d 613, 617 (4th Cir. 2018).

242. *Id.* at 617.

held that plaintiffs were not injured because they had not incurred fraudulent charges nor been denied credit. Accordingly, the district court dismissed the *Hutton* case because plaintiffs failed to satisfy the injury-in-fact requirement to establish standing.[243] On appeal, the Fourth Circuit rejected the district court's ruling that plaintiffs suffered no injury.[244] The circuit court reasoned that plaintiffs had been concretely injured because hackers had used, or attempted to use, the plaintiffs' personal information to open fraudulent accounts.[245] Therefore, the Fourth Circuit in Hutton reversed the district court's ruling and held that plaintiffs' suffered an injury-in-fact to establish Article III standing.[246]

With the *Beck* and *Hutton* cases in the past two years, the Fourth Circuit has struck a middle ground on the issue of standing in data breach cases.[247] The Fourth Circuit distinguished *Hutton* from *Beck* by emphasizing that the *Hutton* plaintiffs were "concretely injured" when accounts were opened in their name, even though fraudulent charges had not occurred. On the other hand, the *Beck* plaintiffs did not have any concrete injury in which their personal

---

243. *Id.* at 618–19.

244. *See id.* at 622.

245. *Id.* ("By way of example, the Hutton Complaint specifies that Hutton received an unsolicited Chase Amazon Visa credit card that was applied for using her social security number and her maiden name (the name that she had provided to the NBEO in 1998). Around the same time, Kaeochinda [a co-plaintiff] learned that someone had applied for a Chase credit card using her social security number and former married name. Mizrahi [a co-plaintiff] also actually received an alert that her credit score had decreased eleven points due to a credit application that was fraudulently filed with Chase, using her address, social security number, and mother's maiden name.").

246. *Id.*

247. Kevin M. McGinty, *Fourth Circuit Decision Seizes Middle Ground on the Issue of Standing in Data Breach Cases*, THE NAT'L L. REV. (June 20, 2018), https://www.natlawreview.com/article/fourth-circuit-decision-seizes-middle-ground-issue-standing-data-breach-cases.

information was misused.[248] Thus, the Fourth Circuit falls in the middle on the standing issue, allowing standing for plaintiffs that suffer misuse of their stolen personal information, but rejecting standing for plaintiffs with an increased risk of future harm after a data breach.[249]

b. Circuit Courts Holding Standing for Increased Risk of Future Harm

i. D.C. Circuit: *Attias v. CareFirst, Inc.*

In 2015 defendant CareFirst, Inc., a group of health insurance companies, experienced a data breach when an intruder breached twenty-two of its computers containing its customers' personal information.[250] Subsequently, seven CareFirst customers brought a class action against CareFirst, Inc.[251] Plaintiffs alleged that the data breach exposed them to a heightened risk of identity theft, and therefore plaintiffs' increased risk of future injury is substantial enough to create Article III standing.[252]

Following the district court's holding that plaintiffs' theory of injury was too speculative to establish standing, the D.C. Circuit reviewed this holding de novo.[253] The D.C. Circuit explained that the main question is whether plaintiffs' complaint plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of

248. Gavejian & Lazzarotti, *supra* note 113.

249. McGinty, *supra* note 247 ("*Hutton* reinforces the Fourth Circuit stance that misuse must accompany the compromise of personal data, but departs from other circuits requiring misuse in that there need not be any pecuniary loss for the misuse to confer standing. The inconvenience of having to rectify fraudulent credit card accounts was deemed sufficient injury to trigger standing. This signals further development of the standing issue in the lower courts which could, over time, influence the Supreme Court to agree to weigh in on this question.").

250. *See* Attias v. CareFirst Inc., 865 F.3d 620, 623 (D.C. Cir. 2017).

251. *Id.* at 623.

252. *Id.* at 626.

253. *Id.* at 625.

CareFirst's alleged negligence in the data breach.[254] Here, CareFirst collects and stores credit card and social security numbers, as well as other personal identification, and personal healthcare information as part of its business.[255] Plaintiffs' complaint alleges that combinations of members' names, birth dates, email addresses, and subscriber identification numbers alone qualifies as personal information, and the unauthorized access to the combination of this information creates a material risk of identity theft for plaintiffs.[256] For example, a cybercriminal could impersonate a victim and obtain medical services in her name, leading to inaccuracies in the victim's medical records, which can cause a host of problems for the victim.[257] The D.C. Circuit agreed with the plaintiffs and held that this constitutes a plausible allegation that plaintiffs face a substantial risk of identity fraud, "even if their social security numbers were never exposed to the data thief."[258]

The D.C. Circuit also clearly distinguished this case from *Clapper*, explaining that in *Clapper* the plaintiff's harm could only occur through a series of contingent events, none of which were alleged to have occurred at the time of the lawsuit.[259] Whereas here, the cybercriminals have already accessed personal identifying data on CareFirst's servers and it is much less speculative to infer that the cybercriminals have the intent and ability to use the data to

254. *Id.* at 627.

255. *Id.* at 627–28.

256. Complaint at 8, Attias v. CareFirst Inc., 865 F.3d 620 (D.C. Cir. 2017) (No. 1:15-cv-00882-CRC).

257. *Id.* For example, it can lead to a victim having inaccuracies in his or her medical record which can cause the victim to receive improper medical care, have his or her medical insurance depleted, become disqualified for health or life insurance, or even become disqualified for some jobs.

258. Attias v. CareFirst Inc., 865 F.3d 620, 628 (D.C. Cir. 2017).

259. *Id.*

harm the victims of the breach.[260] Thus, the risk to plaintiffs here is not based on a long sequence of uncertain certainties; rather, a much more substantial risk than the risk presented to the *Clapper* court exists.[261] Accordingly, the D.C. Circuit held that the claim by the Attias plaintiffs satisfies the injury-in-fact requirement for Article III standing.[262]

ii. Sixth Circuit: *Galaria v. Nationwide Mut. Ins. Co.*

In this case, cybercriminals breached Nationwide's[263] computer network and stole its customers' personal information.[264] Following the breach, plaintiffs Mohammad Galaria and Anthony Hancox brought a putative class action suit.[265] The stolen information included names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers.[266]

The plaintiffs here allege that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft.[267] Plaintiffs further argue that the risk of harm they face is more than the speculative allegations of "possible future injury" or "objectively reasonable likelihood" that the Supreme Court rejected in *Clapper*.[268] The Sixth

---

260. *Id.*

261. *Id.* at 629.

262. *Id.*

263. Nationwide is an insurance and financial services company that maintains records containing sensitive personal information about its customers, as well as potential customers who submit their information to obtain quotes for insurance products. *See* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 386 (6th Cir. 2016).

264. *Galaria*, 663 Fed. App'x at 386 ("On October 3, 2012, hackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others.").

265. *Id.*

266. *Id.*

267. *Id.* at 388.

268. *Id.*

Circuit acknowledges that it is not certain that plaintiffs' data will be misused, however, the increased risk of future harm made it reasonable for plaintiffs to incur mitigation costs.[269] Plaintiffs must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts.[270] For that reason, this is not a case where plaintiffs are manufacturing standing by incurring costs in anticipation of non-imminent harm.[271] Rather, the plaintiffs suffered concrete injuries to mitigate imminent harm from the data breach.[272] Therefore, following this reasoning, the Sixth Circuit held that plaintiffs have suffered a concrete injury and satisfied the injury-in-fact requirement for Article III standing.[273]

iii. Seventh Circuit: *Remijas v. Neiman Marcus Group* and *Dieffenbach v. Barnes & Noble, Inc.*

Remijas v. Neiman Marcus Group

In 2013, cybercriminals hacked Neiman Marcus, a luxury department store, and stole its customers' credit card numbers.[274] Following the breach, Hilary Remijas and

---

269. *Id.* ("Thus, although it might not be 'literally certain' that Plaintiffs' data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable. Where Plaintiffs already know that they have lost control of their data, it would be unreasonable to expect Plaintiffs to wait for actual misuse—a fraudulent charge on a credit card, for example—before taking steps to ensure their own personal and financial security, particularly when Nationwide recommended taking these steps." (citing footnote 5 of Clapper v. Amnesty Intern. USA, 568 U.S. 398 (2013) (citations omitted)).

270. *Id.* Nationwide offered to provide some of these monitoring services for a limited time, but plaintiffs' risk is continuing and they have incurred costs to continue to protect themselves from identity theft. These continued mitigating efforts are needed because following a data breach a reasonable inference can be drawn that the hackers will use the victims' data for fraudulent purposes at some point in the future.

271. *Id.* at 389.

272. *Id.*

273. *Id.*

274. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir.

several others filed complaints against Neiman Marcus and a subsequent class action lawsuit was filed.[275] Following the district court's dismissal for lack of Article III standing, the Seventh Circuit reviewed the ruling de novo.[276]

Plaintiffs claim two imminent injuries: (1) increased risk of fraudulent charges and (2) greater susceptibility to identity theft.[277] Citing *Clapper*, the Seventh Circuit explains that plaintiffs can establish standing for future harm if it is certainly impending.[278] Further, a substantial risk that future injury will occur can establish standing in a data breach case.[279] Accordingly, the Seventh Circuit reasoned that it is plausible to infer that plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach.[280] The Seventh Circuit explained stating, "why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[281] Plaintiffs also claim that they lost time and money protecting themselves from identity theft and fraudulent charges. In addressing this claim, the Seventh Circuit explains that mitigation expenses do not qualify as actual injuries where the harm is not imminent.[282] The Court explains that credit monitoring

2015). Neiman Marcus notified the public of the breach on January 10, 2014, stating that 350,000 credit cards had been exposed to the hackers' malware and 9,200 of those 350,000 credit cards were known to have been fraudulently used.

275. *Id.*

276. *Id.* at 691.

277. *Id.* at 692.

278. *Id.* (Allegations of future harm can establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient." (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013))).

279. *Id.* at 693.

280. *Id.*

281. *Id.*

282. *Id.* at 694 (citing *Clapper*, 133 S.Ct. at 1152).

services come at a price that is more than de minimus[283] and therefore qualifies as a concrete injury.[284] Therefore, the Seventh Circuit held that plaintiffs' injuries associated with resolving fraudulent charges and protection against future identity theft constitute an injury-in-fact under Article III standing requirements.[285]

Dieffenbach v. Barnes & Noble, Inc.

Dieffenbach stems from a 2012 Barnes & Noble data breach where hackers stole customers' personal information.[286] The district court first addressed the standing issue in this case.[287] Citing *Remijas*, the district court held that the *Dieffenbach* plaintiffs satisfied the standing requirement, based on allegations of future substantial risk of identity theft and plaintiffs' lost time and money spent to protect against identity theft.[288] Defendants subsequently appealed to the Seventh Circuit arguing that the case should be dismissed for failing to adequately plead damages.[289]

In addressing the issue on appeal regarding damages, the Seventh Circuit also reaffirmed its position on standing in this case. The Court stated that "[t]o say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are

283. *See, e.g.*, EXPERIAN CREDIT MONITORING, *supra* note 110. Experian credit monitoring costs $4.99 for the first month and then $24.99 for the months following.

284. *Remijas*, 794 F.3d at 694.

285. *Id.* at 695.

286. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018) ([Cybercriminals] acquired details such as customers' names, card numbers and expiration dates, and PINs.").

287. *See In re* Barnes & Noble Pin Pad Litig., 2016 U.S. Dist. LEXIS 137078 (N.D. Ill. Oct. 3, 2016).

288. *See id.* at *9–*11.

289. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018).

available[.]"[290] The Court explained further that plaintiffs have standing on three bases: (1) plaintiffs may have suffered injury from having to pay for credit monitoring services; (2) unauthorized withdrawals that may have caused a loss (the time value of money)[291] even if the bank later restored the principal; or (3) from opportunity cost when an individual has to use his own time to monitor and correct his bank accounts.[292] The Seventh Circuit concluded that these three injuries establish standing and also justify monetary damages.

iv. Ninth Circuit: *In re Zappos.com, Inc.*

In January of 2012 online retailer Zappos.com, Inc. experienced a data breach, where hackers stole the personal information of over 24 million Zappos customers.[293] The plaintiffs in this appeal sued and claimed they established standing based on an increased risk of future identity theft, even though plaintiffs have not alleged instances of actual identity theft or fraud.[294]

The Ninth Circuit evaluated *Zappos* in light of its previous ruling in the 2010 case *Krottner v. Starbucks Corp.* and the 2013 Supreme Court ruling in *Clapper v. Amnesty Int'l USA*. In *Krottner*, a thief stole a laptop containing

---

290. *Id.*

291. *See* Mankiw, *supra* note 110 at 564–65 (explaining the time value of money, of which, at its core, the lesson is that "money today is more valuable than the same amount of money in the future." Therefore, if an individual suffers a fraudulent withdrawal at a bank due to a data breach, if the bank simply restores the account back to its original balance, the individual has lost the amount of interest that could have accrued on the balance due to the time value of money.).

292. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828 (7th Cir. 2018).

293. *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (Cybercriminals "stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information[.]").

294. *See id.* at 1024.

personal information of 97,000 Starbucks employees.[295] The *Krottner* plaintiffs sued, and their only harm to establish standing was an increased risk of future identity theft.[296] The Ninth Circuit in *Krottner* held that this increased risk of future harm was sufficient to establish standing because, with their personally identifiable information in the hands of a hacker, plaintiffs had alleged a credible threat of real and immediate harm.[297] Accordingly, the Ninth Circuit held that *Krottner* is distinguishable from *Clapper* and subsequently followed the reasoning in *Krottner* in this case.[298] Unlike *Clapper*, the plaintiffs' injuries in *Krottner* and *Zappos* do not require a speculative multi-chain link of inferences.[299] Rather, here in *Zappos*, hackers have the means to commit identity theft with plaintiffs' stolen personal information.[300] Therefore, following the ruling in *Krottner*, the Ninth Circuit held that plaintiffs' increased risk of future identity theft established Article III standing.[301]

B. *The Current Privacy Law Landscape*

The second area of unsettled law surrounding data breaches is the current privacy law landscape. As stated

---

295. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).

296. *Id.* at 1142.

297. *Id.* at 1143.

298. *See In re* Zappos.com, Inc., 888 F.3d at 1126.

299. *Id.*

300. *Id.* at 1127 ("Although there is no allegation in this case that the stolen information included social security numbers, as there was in *Krottner*, the information taken in the data breach still gave hackers the means to commit fraud or identity theft, as Zappos itself effectively acknowledged by urging affected customers to change their passwords on any other account where they may have used "the same or a similar password." (citation omitted)). *See also*, *id.* at 1128–29 ("Plaintiffs also specifically allege that '[a] person whose PII has been obtained and compromised may not see the full extent of identity theft or identity fraud for years.' And 'it may take some time for the victim to become aware of the theft.'").

301. *Id.* at 1128.

previously, there are fifty separate data breach notification statutes, all with varying degrees of severity.[302] In addition to these notification statutes, two significant privacy laws were enacted in the past year. These laws are: (1) the General Data Protection Regulation (GDPR)[303] and (2) the California Consumer Privacy Act (CCPA).[304] These laws have a significant impact on organizations and individuals throughout the world. As U.S. citizens and lawmakers begin to realize the gravity of security breaches, these two laws will provide an example for the U.S. Congress and pave the way for a uniform federal privacy law.

1. The General Data Protection Regulation (GDPR)

The world's strongest data protection rules were passed into law when the General Data Protection Regulation was adopted by the European Parliament and the European Council in April 2016.[305] Following the ratification of the GDPR, there was a two-year transition period to allow organizations to adapt to the new rule and change their methods, policies, procedures, and documentation to meet the new requirements.[306] Then, on May 25, 2018, the GDPR came into full force and covered organizations are now required to comply with the GDPR in its entirety or face penalty.[307]

The GDPR intended to "harmonize" data privacy laws in

302. *See supra* pp. 1139–42 and accompanying notes.

303. Commission Regulation 2016/679, 2016 O.J. (L119) [hereinafter GDPR].

304. California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798 (2018) [hereinafter CCPA].

305. GDPR, *supra* note 303. *See also* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Jan. 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

306. BALLON, *supra* note 169, at § 26.04[18][A].

307. *See* Francoise Gilbert, *Global Privacy and Security Law*, Ch. 6A "EU Data Protection Regulation" (Wolters Kluwer Law & Business Publishing).

Europe as well as protect and empower all EU citizens' data privacy.[308] The GDPR advanced these intentions by creating eight rights for individuals regarding personal information security.[309] The most notable rights created are the right to be forgotten, which allows an individual to have its personal information removed from an organization; the right to access, which gives individuals the right to know exactly what information is held about them and how it is processed; and the right to be informed, which requires all organizations to be completely transparent in how they are using personal data.[310] Outside of the eight individual rights, the GDPR also protects individuals by requiring all companies that collect or process EU citizens' personal data to appoint a data protection officer.[311] The data protection officer at each company is responsible for overseeing the data protection strategy and implementation to ensure compliance with GDPR requirements.[312]

---

308. EU GDPR, https://eugdpr.org/ (last visited Feb. 24, 2019).

309. INFO. COMM'RS OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ (visited Feb. 24, 2019) (These eight rights for individuals include: (1) the right to be informed; (2) the right of access; (3) the right to rectification; (4) the right to erasure; (5) the right to restrict processing; (6) the right to data portability; (7) the right to object; (8) rights in relation to automated decision making and profiling.).

310. *See id.*

311. GDPR, *supra* note 303, at art. 37.

312. Nate Lord, *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019*, DIGITAL GUARDIAN (Jan. 23, 2019), https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance. The data protection officer's responsibilities include, but are not limited to, the following:

> Educating the company and employees on important compliance requirements;
> Training staff involved in data processing;
> Conducting audits to ensure compliance and address potential issues proactively;
> Serving as the point of contact between the company and GDPR Supervisory Authorities;
> Monitoring performance and providing advice on the impact of data

Arguably, the most significant regulation from the GDPR is the high standard it created for notifying individuals after a breach. The GDPR requires an organization to notify the relevant regulator within seventy-two hours of discovering the data breach.[313] This notification must include a description of the nature of the breach, the estimated impact of the breach, the name and details of the data protection officer, and a description of the measures taken by the organization to address the breach.[314] Finally, noncompliance with any of the GDPR regulations will result in significant fines.[315] The GDPR fines are a tiered system with lower tier fines of €10 million or 2% of annual revenues, whichever is greater, for noncompliance of Articles 8, 11, 25–39, and 41–43.[316] The higher tiered fines are €20 million or

---

protection efforts;
Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request.

Id.; *see also* GDPR, *supra* note 303, at art. 37.

313. GDPR, *supra* note 303, at art. 33(1). ("In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.").

314. GDPR, *supra* note 303, at art. 33(3).
The notification referred to in paragraph 1 shall at least:
1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. describe the likely consequences of the personal data breach;
4. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
Id.

315. *See* GDPR, *supra* note 303, at art. 83.

316. *See id.* at art. 83(4). ("Infringements of the following provisions shall, in

4% of annual revenues, whichever is greater, for noncompliance of Articles 5, 6, 7, 9, 12–22, and 44–49.[317] As a result, these fines create a large incentive for companies to stay diligent and comply with all GDPR regulations.

Although the GDPR has significantly increased protection for individuals and their personal information, it is not perfect nor without criticism.[318] One criticism of the GDPR is that it does not even achieve its goal of harmonizing all of the data protection laws in the EU.[319] Of the sixty-five articles that relate to the rights of data subjects, thirty of them allow member states to engage in variation from the standard set in the GDPR.[320] Accordingly, there is the potential that multiple member states will deviate from the norm and thereby destroy the harmonization of all data

---

accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4).").

317. *See id.* at art. 83(5). ("Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).").

318. David Bender, *GDPR Harmonization: Reality or Myth?*, IAPP: PRIVACY PERSPECTIVES (June 7, 2018), https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/.

319. *See id.*; *see also* Katie Nolan, *GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law*, Berkeley TECH. L. J. BLOG (Jan. 20, 2018), http://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/.

320. Bender, *supra* note 318.

protection laws in the EU.[321] As a result, the GDPR will not achieve its goal of having a "single set of rules" allowing businesses to save costs on compliance.[322] Just the opposite has occurred. Therefore, the GDPR will not achieve harmonization if member states continue to deviate, thereby making compliance more burdensome and costly for businesses.[323]

The GDPR's failure to achieve harmonization adds to the already concerning problem that GDPR compliance is too burdensome on organizations and the extremely costly penalties will have detrimental consequences on business.[324]

---

321. *Id.* ("National legislation is needed to select among the variations permitted in the GDPR itself. At this writing, only a minority of member states have enacted this implementing legislation—although all 28 were to have it in place by May 25, 2018—and some others have draft legislation. We do not yet know the degree of diversity that will actually be introduced by selecting variations, but the potential for diversity is great. After all, the fact that a diversion from the norm is included in a particular article suggests that there may have been at least one member state that lobbied for it.").

322. *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses,* European Commission Press Release IP/12/46 (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm (This 2012 proposal aimed for the GDPR to be a "single law [that] will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year.").

323. *See* Nolan, *supra* note 319 (arguing that in the future national data protection laws will continue to diverge). ("The EU legislature's aim to create a single set of rules has not come to fruition. While there is a great deal more convergence on the substance of EU data protection law compared to under the Data Protection Directive, it is by no means a complete harmonization. The practical reality is that national data protection laws will continue to diverge. While a complex co-operation and consistency mechanism has been designed to determine the division of responsibilities between data protection authorities, the GDPR is silent as to when the national data protection legislation will apply. In the absence of any applicable law rule, organizations will face considerable uncertainty as to their legal obligations.").

324. *See* Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, HARV. BUS. REV. (April 9, 2018), https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain; Daphne Keller, *The New, Worse 'Right to be Forgotten'*, POLITICO EU (Jan. 27, 2016 7:28 PM), https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/ (Daphne Keller, former associate general counsel at Google criticizes the "right to be forgotten."); *see also*

Many in the technology industry fear that the GDPR's strict regulations could push small and medium-sized competitors out of the industry.[325] This is because companies spent hundreds of hours becoming compliant with the GDPR, costing many companies over $1 million dollars.[326] Accordingly, compliance alone is extremely time-consuming and costly for small and medium-sized businesses.[327] Then, if a company slips up and is found non-compliant, it will face an enormous fine under Article 83.[328] In sum, this time and money spent on compliance with the GDPR takes away valuable resources that a company could be using to grow its business. Therefore, it is a legitimate and well-founded fear that the GDPR's strict regulations could cause small and

---

In GDPR Compliance, U.S. Companies Lag Behind United Kingdom, EU, CORP. COUNSEL (July 12, 2018) (criticizing the cost of complying with the GDPR).

325. Caroline Spiezio, *An American GDPR? Companies' Privacy Gurus Discuss Future Federal Data Law in DC*, CORP. COUNSEL (Sept. 26, 2018 3:57 PM), https://www.law.com/corpcounsel/2018/09/26/an-american-gdpr-companies-privacy-gurus-discuss-future-federal-data-law-in-d-c/.

326. *See id.* (quoting Google's chief privacy officer Keith Enright stating that "Google's preparations for GDPR had taken 'hundreds of years of human time,' time smaller companies may not have to spare."); *see also* Dan Clark, *In GDPR Compliance, US Companies Lag Behind United Kingdom, EU*, CORP. COUNSEL (July 12, 2018 1:23 PM), https://www.law.com/corpcounsel/2018/07/12/in-gdpr-compliance-u-s-companies-lag-behind-united-kingdom-eu/ ("Twenty-five percent of U.S. respondents spent over $1 million on becoming compliant with the GDPR.").

327. *See* Spiezio, *supra* note 325. *See also Hearing on Protecting Consumer Privacy in the Era of Big Data Before the H. Comm. On Energy and Commerce and S. Comm. On Consumer Protection and Commerce*, 116th Cong. (2019) (statement by Roslyn Layton, Visiting Scholar, THE AM. ENTER. INST.) ("There is little to no data that shows that small to medium sized companies are growing in the EU as a result of the regulation. The European Commission's Digital Scoreboard reports shows a consistent lag in the SME [small to medium enterprise] segment, particularly to modernize their websites and market outside their own EU countries. One study suggests that small- and medium-sized ad tech competitors have lost up to one-third of their market position since the GDPR took effect. [. . .] The GDPR is a barrier to market entry that punishes small firms, rewards large ones, and creates a cozy relationship between regulators and the firms they regulate." (footnotes omitted)).

328. *See* GDPR, *supra* note 303, at art. 83.

medium-sized businesses to fail.

2. The California Consumer Privacy Act

Following the lead of the EU's GDPR, California enacted the most comprehensive privacy law in the United States when it passed the California Consumer Privacy Act (CCPA) in June 2018.[329] The law does not go into effect until January 1, 2020, which allows companies to adapt to the changes in the law.[330] Similar to the GDPR, the CCPA creates new data privacy rights for California consumers. These data privacy rights include the rights to know, access, delete, and opt out of the sale of personal information.[331] Also similar to the GDPR, the CCPA imposes penalties on companies that violate the law. If a company is found in violation of the CCPA, it will have thirty days to cure any violation after being notified of the alleged noncompliance.[332] Then, if a company fails to cure any violation within thirty days, it can face a civil penalty up to $7,500 for every intentional violation.[333] Additionally, the CCPA provides consumers a private right of action that allows consumers, either individually or as a class, to seek statutory or actual damages and injunctive relief, if their personal information is subject to unauthorized access.[334]

Unlike the GDPR, the CCPA does not apply to all businesses in the United States, nor all the businesses in California. First, the CCPA only applies to for-profit

329. CCPA, *supra* note 304.

330. *See* Mark G. McCreary, *The California Consumer Privacy Act: What You Need to Know*, N. J. L. J. (Dec. 1, 2018 10:00 AM), https://www.law.com/njlawjournal/2018/12/01/the-california-consumer-privacy-act-what-you-need-to-know/.

331. CCPA, *supra* note 304, at §§ 1798.100–1798.120.

332. *Id.* at § 1785.155.

333. *Id.* at § 1785.155.

334. *Id.* at § 1798.150.

organizations that conduct business in California.[335] Second, for the CCPA to apply, an organization must satisfy at least one of the following three criteria: (1) have an annual gross revenue in excess of $25 million; (2) receive or disclose the personal information of 50,000 or more California residents, households or devices on an annual basis; or (3) derive fifty percent or more of their annual revenues from selling California residents' personal information.[336] Therefore, the CCPA provides strict rules for large for-profit organizations doing business in California but does not apply these rules to small businesses or non-profit organizations.

Another difference between the GDPR and CCPA is that the CCPA does not provide a data breach notification requirement. Rather, the California legislature chose to continue with its own data breach notification statute that has been the law since 2003.[337] This notification law requires that an organization notify customers of a data breach and specifically sets forth the manner in which an organization is to notify those affected by the breach.[338] However,

---

335. *See* McCreary, *supra* note 330.

336. CCPA, *supra* note 304, at § 1798.140(c).

337. *See* CAL. CIV. CODE 1798.82.

338. *Id.* at 1798.82(d).

> A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
>
> (1) The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
>
> (A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.
>
> (B) The title and headings in the notice shall be clearly and conspicuously displayed.
>
> (C) The text of the notice and any other notice provided pursuant to this

California's data breach notification law does not provide a time requirement to notify individuals of a data breach, rather it simply requires disclosure "be made in the most expedient time possible and without unreasonable delay[.]"[339] Therefore, the California legislature punted the opportunity to clarify the required time for an organization to notify individuals of a data breach.

The CCPA has been praised for providing better data protection to California residents but also criticized by businesses that will need to comply with the law.[340] The main concern is that the law is much too broad and ambiguous. Namely, the CCPA's definitions of "business" and "personal information" are criticized.[341] The CCPA's definition of "business" is a concern because, as presently written, the CCPA could not only apply to organizations that sell individuals' data for financial gain but also any website that collects IP addresses from millions of unique visitors each day.[342] Accordingly, this broad definition could pull in a website that does not conduct business in California but simply has a website that collects IP addresses from its visitors in California. As a result, this will put an enormous burden on these websites to comply with a law that they did

---

section shall be no smaller than 10-point type.

Id.

339. *Id.* at 1798.82(a).

340. Allison Grande, *Don't Water Down Calif. Privacy Law, Lawmakers Told*, LAW360 (Dec. 5, 2018), https://www.law360.com/articles/1108475/don-t-water-down-calif-privacy-law-lawmakers-told (reporting that many advocacy groups applaud the law for being a "privacy leader" in America). Whereas, others in industry criticized portions of the law. *Id.* ("The California Chamber of Commerce and other business groups from a range of industry sectors in August asked lawmakers to rein in some of the more 'unworkable' aspects of the statute, including its broad definition of personal information and its application to a wide range of data uses.").

341. *See* CCPA, *supra* note 304, at § 1785.140(c), (o).

342. Danny Allan, *California's New Data Privacy Law Could Begin a Regulatory Disaster*, FORTUNE (Oct. 23, 2018), https://fortune.com/2018/10/23/california-data-privacy-law-gdpr/.

not foresee.

A concern greater than the CCPA's definition of business is the law's enormously broad definition of "personal information."[343] Under the CCPA's definition of personal information, the law is not limited to a company's customers. Essentially, if a company physically or virtually touches a California resident, it will be subject to the CCPA.[344] Under the CCPA, the term "personal information" includes any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or household*."[345] This overly broad definition of personal information includes any information that could be linked with a person, which essentially is all information.[346] This makes the entire compliance with the CCPA very confusing for American businesses. Although this broad definition was intended to protect as much consumer personal information as possible, it could actually "undermine important privacy-protective practices like encouraging companies to handle data in a way that is not directly linked to a consumer's

343. *See* CCPA, *supra* note 304, at § 1785.140(o).

344. *See Landmark New Privacy Law in California to Challenge Businesses Nationwide*, JD SUPRA (July 5, 2018), https://www.jdsupra.com/legalnews/landmark-new-privacy-law-in-california-99847/ (The CCPA encompasses all California residents, including employees, customers, visitors to a company internet site or business location, contractors and independent contractors, and vendors.).

345. *See* CCPA, *supra* note 304, at § 1785.140(o)(1)(A); *see also* CCPA, *supra* note 304, at § 1785.140(o)(1)(B)–(K) (Personal information under the CCPA includes but is not limited to: records of personal property; products or services purchased, obtained, or *considered*; other purchasing or consuming histories or tendencies; biometric information; internet or other electronic network activity information (e.g., browsing and search history, and information regarding an individual's interaction with a website, application, or advertisement); geolocation data; and professional or employment-related information.).

346. Spiezio, *supra* note 325. ("CCPA's definition of 'personal information' goes beyond information that actually identifies a person to include any information that 'could be linked with a person,' which arguably is all information." (quoting Amazon's Vice President and Associate General Counsel Andrew Devore)).

identity."[347] Therefore, the CCPA's broad definition of "personal information" will make compliance with the law burdensome and costly, and potentially reduce data protection for California residents.

V. PROPOSED SOLUTION: SUPREME COURT ADDRESSING CIRCUIT SPLIT AND A FEDERAL PRIVACY LAW

Current U.S. laws have failed to protect consumers and facilitate stronger cybersecurity efforts. The ambiguous and complex regulatory environment of cybersecurity law has created a host of problems for both consumers and U.S. businesses. These issues, as well as the increased prevalence of data breaches, make it clear that change is needed to make laws more effective and provide better protection for consumers. This Comment proposes two changes in the law as a solution. The first change is for the Supreme Court to provide a clear rule on Article III standing in a data breach case. The second change is for Congress to pass a uniform federal privacy law. The following subsections will explore how these two changes will improve consumer protection by providing incentives for companies to take action and protect consumers both before and after a data breach.

A. *Supreme Court Ruling Addressing Article III Standing in Data Breach Class Action Cases*

The current circuit split on Article III standing in data breach cases leaves consumers with an uphill battle to hold the company which neglected to protect their personal information liable.[348] Therefore, the first action that can be taken is for the Supreme Court to follow the D.C., Sixth, Seventh, and Ninth Circuits and allow the increased risk of future injury to constitute an injury-in-fact for Article III

347. *Id.*

348. *See supra* Section II.B.

standing.[349]

The Supreme Court may have this opportunity with the class action lawsuits filed against Equifax. The facts surrounding the Equifax data breach coincide with the rulings in *Attias*, *Galaria*, *Remijas*, and *Zappos*. In each of those cases, the circuit court held that the threat of future harm from identity theft was sufficient to establish Article III standing.[350] Additionally, in those cases, cybercriminals hacked into each defendant company's system to steal personal information of its customers such as names, dates of birth, Social Security numbers, and driver's licenses.[351] These circuit courts all held that the threat of future harm resulting from the breach and the costs of mitigating future damages constituted an injury-in-fact for Article III standing.[352] Similarly, with the Equifax breach, cybercriminals stole names, Social Security numbers, birth dates, addresses, and driver's license numbers.[353] Therefore, the victims of the Equifax data breach also have a threat of future harm resulting from the data breach and will incur costs to mitigate damages such as credit monitoring.[354]

The rulings in *Attias*, *Galaria*, and *Remijas* also provide logical legal reasoning for why increased risk of future injury constitutes an injury-in-fact. First and foremost, the entire purpose of a hack is to make fraudulent charges or assume

---

349. *See* Attias v. CareFirst Inc., 865 F.3d 620, 629–30 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390–91 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 698–97 (7th Cir. 2015).

350. *See Attias*, 865 F.3d at 629–30; *Galaria*, 663 F. App'x at 390–91; *Remijas*, 794 F.3d at 698–97.

351. *See Attias*, 865 F.3d at 629–30; *Galaria*, 663 F. App'x at 390–91; *Remijas*, 794 F.3d at 698–97.

352. *See Attias*, 865 F.3d at 629–30; *Galaria*, 663 F. App'x at 390–91; *Remijas*, 794 F.3d at 698–97.

353. EQUIFAX, *supra* note 2.

354. *See* Villadiego, *supra* note 133; EXPERIAN CREDIT MONITORING, *supra* note 110.

consumers' identities at some point.[355] A cybercriminal's motive for hacking a system is to use the stolen information for their benefit or to sell it to others who can also use the information to make fraudulent charges.[356] Therefore, an injury is "certainly impending" for a consumer whose data has been breached, satisfying the immanency requirement for an injury-in-fact under Article III standing.[357] Additionally, any rational consumer would take the proper steps to protect themselves from future harm after a breach by monitoring their credit, checking their bank statements, and modifying their financial accounts. As stated previously, these mitigation efforts are not free[358] and but for the data breach, consumers would not incur the additional costs to monitor their credit and other financial information.[359] Accordingly, these costs are certainly an actual injury that satisfies the "concrete and particularized" requirement for Article III standing.[360] Therefore, it is sound law and logical

355. *Remijas*, 794 F.3d at 693.

356. Kristen L. Burge, *Your Data Was Stolen, But Not Your Identity (Yet)*, ABA (Jan. 11, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/your-data-was-stolen-not-your-identity-yet/ ("A majority of circuits reason that 'there is a "certainly impending" threat that the affected individuals will be the victims of financial or identity fraud. After all, the motive of the hackers is to use the stolen information for their own benefit or to sell it to others,' explains Newby. These circuits apply common sense to data breach cases, Newby suggests. 'The entire purpose of hacking a company to swipe thousands of credit card numbers or personal identifiers is to misuse that information for gain, like making fraudulent purchases or engaging in tax refund fraud or identity fraud. Why should the people whose information was compromised have to wait until that happens before getting some relief?'" quoting Tyler G. Newby co-chair of the ABA Section of Litigation's Privacy & Data Security Committee); s*ee also* Villadiego, *supra* note 133 (discussing how cybercriminals will use the information stolen in the Equifax data breach).

357. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013).

358. *See* EXPERIAN CREDIT MONITORING, *supra* note 110.

359. *See Remijas*, 794 F.3d at 693.

360. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016). *See also Remijas*, 794 F.3d at 694 (holding that credit monitoring following a data breach constitutes a concrete injury); *Galaria*, 663 Fed. App'x at 389 (holding that plaintiffs suffered concrete injuries to mitigate imminent harm from the data

thinking for the Supreme Court to hold that the victims of the Equifax data breach have suffered an injury-in-fact under Article III standing requirements. If the Supreme Court is able to rule on the Article III standing requirements in a data breach case, it will bring clarity to the law and allow victims of a data breach to have their day in court. This will give data breach victims the opportunity to hold the company that did not protect their personal information liable.

In addition to giving data breach victims their day in court, allowing for Article III standing in a data breach case will incentivize companies to improve their cybersecurity efforts to prevent future data breaches. Although some argue that class action lawsuits do not act as a deterrence,[361] there is sound rationale and evidence that class actions deter companies from bad behavior.[362] Allowing for Article III standing in data breach cases based on the threat of future injury will lead to more class action cases against companies that have their data breached. The threat of future class action litigation will then act as a general deterrence[363] for

---

breach).

361. *See* Linda S. Mullenix, *Ending Class Actions as We Know Them: Rethinking the American Class Action*, 64 EMORY L.J. 399, 420–21 (2014).

362. Fitzpatrick, *supra* note 14. Fitzpatrick explains the legal theory of deterrence and provides evidence that class actions deter wrongdoing. In a 1981 study, economists found that settlements from class actions for price fixing were 10 times greater than government imposed fines and that a deterrent effect came from the threat of an award of private treble damages (citing Michael Kent Block et al., *The Deterrent Effect of Antitrust Enforcement*, 89 J. OF POL. ECON. 429, 441 (1981). Additionally, a recent study in 2010 of American securities fraud class action lawsuits found that class action lawsuits induced companies to be more forthcoming to their shareholders (citing James P. Naughton et al., *Private Litigation Costs and Voluntary Disclosure: Evidence From the Morrison Ruling*, (May 2014) (unpublished paper on file with Kellog School of Management, Working Paper updated February 2017))).

363. Fitzpatrick, *supra* note 14. General deterrence refers to how potential wrongdoers respond to a potential lawsuit—that is, do potential wrongdoers decide not to commit misconduct to begin with because they are afraid of lawsuits against them? Whereas, specific deterrence is how an actual wrongdoer responds to an actual lawsuit against it—that is, does the actual wrongdoer stop the misbehavior after it is caught?

these companies. The theory of general deterrence assumes that people, and therefore people running companies, are rational and that a rational person does not want to be sued.[364] With a lawsuit, a company will have to pay its own lawyers and the plaintiff if it loses in court.[365] Therefore, if the misbehavior benefits the corporation less than the harm it inflicts on others, then the corporation will rationally choose not to engage in the misconduct.[366] Consequently, under the theory of general deterrence, the only time a corporation will rationally choose to engage in misconduct is when the benefits outweigh the harm.[367]

In the context of data breaches, companies are not engaging in deliberate misconduct per se. Rather, companies are not putting the proper protections in place to adequately protect their customers' sensitive personal information. Applying the general deterrence theory to data breaches means that class action litigation needs to deter companies by having the cost of a class action lawsuit outweigh the cost of putting in place more cybersecurity protections.[368] Currently, there is not enough general deterrence for organizations in America because the law is inconsistent regarding Article III standing and not every circuit allows for standing based on the threat of future harm.[369] Therefore, companies do not always have to pay for costly class action litigation or treble damages if they lose in court because the class action case does not even make it to the courtroom without Article III standing. In short, there is not enough incentive for companies to improve their consumer data protection efforts because some circuits do not allow for

364. *Id.*

365. *Id.*

366. *Id.*

367. *Id.*

368. *See id.*

369. *See* Beck v. McDonald, 848 F.3d 262, 277–78 (4th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017).

Article III standing when a breach occurs.

If the Supreme Court were to resolve the current circuit split and rule that increased risk of future harm from a data breach satisfies the Article III standing requirements, it would allow more consumers to file class actions that survive a motion to dismiss and actually make it to discovery. This will provide an initial remedy for breached consumers because they will be able to hold the company that did not protect their data accountable. Additionally, it will make litigation costlier for companies that experience a breach because they will no longer be able to win on a motion to dismiss. Then, applying the theory of general deterrence, more lawsuits will incentivize companies to improve their cybersecurity efforts to better protect consumer information because the potential cost of litigation will outweigh the cost of protecting consumer information.[370] As a result, the companies' improved cybersecurity and consumer protection efforts will lead to achieving the ultimate goal of preventing data breaches in the first place so that consumers' personal information is not stolen and in the hands of cybercriminals.

B. *A Federal Data Breach Notification Law*

The infamous Equifax data breach and the overall rise in data breaches has led to many lawmakers to call for a federal data breach law.[371] Likewise, the recent passing of

370. *See supra* notes 366–67 and accompanying text.

371. *See* S. 2289 115th Cong. (2d Sess. 2018) (Senators Elizabeth Warren (Mass.) and Mark Warner (Va.) introduced the bill "Data Breach and Compensation Act" fining companies $100 for each consumer whose information is compromised and adding an additional $50 fine if the company failed to notify officials in a timely manner). *See also* S. 2197 115th Cong. (1st Sess. 2017) (Senators Richard Blumenthal (CT), Bill Nelson (FL), and Tammy Baldwin (WI) introduced a bill titled "Data Security and Breach Notification Act." This bill would require, among other things, notification of the affected parties within thirty days and notification to law enforcement if the breach involves more than 10,000 individuals); The Application Privacy, Protection, and Security Act of 2018, H.R. 6547 115th Cong. (2018) (this law would govern how data is collected

the GDPR and CCPA has led those in industry to call for a uniform federal privacy law to ease the compliance burden in the United States.[372] Therefore, the United States Federal Government can follow the lead of the European Union and California by creating a comprehensive federal privacy law. The Federal Government can use the GDPR and CCPA as an example by adopting the successful provisions of those laws, while also improving upon the unsuccessful provisions that garnered significant criticism.[373]

After analyzing American cybersecurity issues, as well as the GDPR and CCPA, there are five necessary provisions to be included in a U.S. federal privacy law. Accordingly, a U.S. federal privacy law must: (1) establish the data rights of all American citizens; (2) clearly define terms within the privacy law; (3) include a comprehensive data breach notification requirement; (4) truly be harmonized and

---

and secured on mobile devices); The Data Care Act of 2018 S. 3744 115 Cong. (2d Sess. 2018) (Introduced by Senator Brian Schatz (Haw.), this bill would require companies to use reasonable care when collecting data and places restrictions on how data can be shared.).

372. *See* Dan Clark, *A PLEA FOR PROTECTION; Will a federal data privacy law save the day?*, CORP. COUNSEL (Feb. 1, 2019), https://www.law.com/corpcounsel/2019/02/04/a-plea-for-protection-will-a-federal-data-privacy-law-save-the-day/?slreturn=20190609162321 (reporting that Intel, Alphabet Inc. (Google), and IBM have all weighed in on a federal privacy law in the United States); *see also* Cat Zakrzewski, *The Technology 202: More than 200 companies are calling for a national privacy law. Here's an inside look at their proposal*, WASH. POST (Dec. 6, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2018/12/06/the-technology-202-more-than-200-companies-are-calling-for-a-national-privacy-law-here-s-an-inside-look-at-their-proposal/5c0819be1b326b60d128012e/?noredirect=on&utm_term=.dc52e58ebfc9 (stating that the Business Roundtable, a group of more than 200 retailers, tech companies, and financial institutions, call on the U.S. to adopt a national privacy law that would apply the same data collection requirements to all companies regardless of sector.); *Tim Cook calls for US federal privacy law to tackle 'weaponized' personal data*, THE GUARDIAN (Oct. 24, 2018), https://www.theguardian.com/technology/2018/oct/24/tim-cook-us-federal-privacy-law-weaponized-personal-data (stating that Apple's CEO Tim Cook, Facebook's CEO Mark Zuckerburg, and Google's CEO Sundar Pichai, all support a federal privacy law in the U.S.).

373. *See supra* Section IV.B.

uniform across the United States; and (5) the law must have a reasonable and just penalty for noncompliance. By incorporating all five of these provisions in a federal privacy law, the United States will ensure that cybersecurity efforts in America are improved and consumers' private information is better protected in the future.

The first necessary provision for a U.S. federal privacy law is a provision establishing the data rights of all American citizens. Similar to the GDPR and CCPA, a U.S. federal privacy law needs to establish basic data rights for all of its citizens.[374] At the very least, a federal privacy law should give U.S. residents the right to be informed as to how companies are using their personal information, the right to have their data amended or deleted, and ensure that their data is not being collected and shared without their consent.[375] As a result, this provision will give Americans more freedom and control of their personal information before and after it is collected by an organization.

Second, a federal privacy law must clearly define its terms. Namely, a U.S. federal privacy law must clearly define the term "personal information," which is something the GDPR and CCPA failed to accomplish.[376] This will make compliance with the law much less confusing and costly. Accordingly, this law will not drive out small and medium-

374. *See id.*

375. *See* David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law/; *see also Hearing on Protecting Consumer Privacy in the Era of Big Data Before the H. Comm. On Energy and Commerce and S. Comm. On Consumer Protection and Commerce*, 116th Cong. (2019) (statement by Denise E. Zheng, Vice President, Technology and Innovation, Business Roundtable) (stating that at the heart of the Business Roundtable proposal is a set of core individual rights that they believe all consumers should have, including the right to transparency regarding a company's data practices, consumers' right to exert control over their data, the right to access and correct inaccuracies in personal data about them, and the right to delete personal data).

376. *See supra* notes 343–347 and accompanying text (explaining the issues with the GDPR and CCPA's definition of "personal information").

sized businesses with its large compliance costs. Additionally, a clear definition of personal information will enable organizations to continue to perform important privacy-protection practices. The second term that must be clearly defined in a U.S. federal privacy law is the term "business."[377] This will allow each business in America to know whether or not it must comply with the law. Again, this will lower compliance costs because organizations will know whether or not they must comply with the law and plan accordingly. In the aggregate, clearly defined terms in a U.S. federal data breach notification law will allow organizations to comply with the law in an efficient manner and ensure that consumers' personal information is protected.

Third, and arguably most importantly, a U.S. federal privacy law must have a comprehensive data breach notification provision. Taking from the GDPR, this data breach notification clause must have a time-limit requiring organizations to notify the proper authorities within seventy-two hours of the breach.[378] However, this provision would only require notification that the breach occurred and not require a full investigation yet. This will prevent a company and its executives from engaging in any bad behavior such as insider trading before the breach is made public.[379] Additionally, it will put the government on notice of the

377. *See supra* notes 341–42 and accompanying text (explaining the issues with the CCPA's definition of "business").

378. *See supra* pp. 1180–81 and accompanying notes (explaining the GDPR's 72-hour notification requirement); *see also* 23 NYCRR § 500.17 (This New York State Department of Financial Services regulation requires financial organizations to give notice to the New York State Superintendent of Financial Services within 72 hours of identifying that a cybersecurity event has occurred.). A federal data breach notification law mirroring these statutes would ensure that all consumers are informed of a data breach properly and reduce the ability for corporate executives to misbehave, such as by selling securities of a corporation before notifying the public of the breach.

379. *See supra* pp. 1152–53 and accompanying notes (discussing the investigation into Equifax's executives for potential insider trading violations following the infamous 2017 breach).

breach, but not be overly burdensome for companies because they will not have to do a full investigation of the breach within just seventy-two hours. Therefore, following notification of the proper government authorities, an organization can do a full investigation into the breach with oversight from the government.

Then, a U.S. federal privacy law must also incorporate a time-limit in which a company must notify the consumers affected by the breach. Congress can conduct research to determine the appropriate amount of time, but an analysis of the current state data breach notification laws shows that requiring notification within thirty days of a breach to affected consumers would be appropriate.[380] This thirty-day time limit will give an organization ample time to conduct a full investigation. Additionally, this requirement will ensure that consumers are notified of a breach in a timely manner so they can take the proper steps to mitigate any losses and protect their personal information from further exposure to cybercriminals through credit freezes, credit monitoring, and the like.[381] Combined, these two notification requirements will give government notice of a breach to police any bad behavior by the breached organization, as well as allow the organization to conduct a full investigation of the breach and then notify the affected individuals in a timely manner.

The fourth requirement of a data breach notification provision in a U.S. federal privacy law would be a uniform manner in which individuals are notified. As such, a U.S. federal privacy law must be truly harmonized. The GDPR tried to harmonize the data privacy laws in the EU, but, as stated previously, the GDPR failed to do so.[382] The United States should take this opportunity to create a uniform federal privacy law that will preempt the fifty separate state

380. *See supra* notes 83–86 and accompanying text.

381. *See supra* note 109 and accompanying text.

382. *See supra* pp. 1178–80 and accompanying notes.

privacy laws.[383] As stated prior, the fifty separate data breach notification laws are a compliance nightmare for organizations in America.[384] All fifty of these notification laws have different requirements for the manner in which organizations must notify individuals affected by a breach. A proposed solution is to require organizations to inform individuals affected by a breach via an email, phone call, and a letter in the mail. This will ensure that all affected individuals are notified of the breach because the majority of Americans utilize either email, physical letters, or telephones. In addition, an organization that experiences a security breach will no longer need to comply with fifty separate data breach notification laws, rather, it will only need to look to one federal privacy law for all of its notification requirements. Therefore, a truly harmonized federal privacy law will ease the compliance burdens for organizations and allow these organizations to focus on data protection rather than simply compliance with a vast amount of privacy laws.[385]

Finally, the fifth requirement for a federal U.S. privacy law is that it must have a reasonable and just penalty for noncompliance. The penalty for violating a federal U.S. privacy law will act as a specific deterrent to organizations that violate the law.[386] Specific deterrence refers to the

---

383. Jedidiah Bracy, *In Push for U.S. Federal Privacy Law, State Preemption Will Depend on the Details*, IAPP: THE PRIVACY ADVISOR (Sept. 27, 2018), https://iapp.org/news/a/in-push-for-us-federal-privacy-law-state-preemption-will-depend-on-the-details/; *see also Hearing on Protecting Consumer Privacy in the Era of Big Data Before the H. Comm. On Energy and Commerce and S. Comm. On Consumer Protection and Commerce*, 116th Cong. (2019) (statement by David F. Grimaldi, Jr., Executive Vice President, Public Policy, Interactive Advertising Bureau) (arguing that a U.S. federal privacy law "should reduce consumer and business confusion by preempting the growing patchwork of state privacy laws.").

384. *See supra* pp. 1139–42 and accompanying notes.

385. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

386. *See* Fitzpatrick, *supra* note 14, at 184. The threat of class action litigation

effects of enforcement against a particular violator on that violator's future conduct.[387] Applying specific deterrence to a federal privacy notification law would entail punishments on an organization for violating specific provisions of the law. Therefore, the punishment to a company for violating the U.S. federal privacy law would act as a specific deterrent to that violating organization. Specific deterrence would shape that violating company's behavior to come into compliance with the law for fear of being penalized again. As a result, consumer personal information is better protected because this company is now in compliance with the law and properly protecting its customers' data.

However, the punishment for noncompliance with a federal U.S. privacy law cannot be so severe that it completely wipes out some businesses. With the GDPR's fines starting at €10 million or €20 million depending on which article is violated, there is serious concern that these enormous fines could push small businesses out of the EU.[388] With 30.2 million small businesses in the United States, small businesses make up 99.9% of all business in the United States.[389] Additionally, United States small businesses employed 58.9 million people, or 47.5% of the workforce, in

from a data breach will act as a general deterrent and force organizations to improve their cybersecurity efforts to protect against a data breach. *See also supra* Section V.A. Whereas, a federal U.S. privacy law will act as a specific deterrent for companies, deterring them from violating the federal privacy law.

387. SEAN FARHANG, THE LITIGATION STATE, 8–9 (2010). Farhang explains that there is considerable evidence that private lawsuits are an effective tool in shaping the behavior of both private entities and governmental subunits. Farhang also notes the aspect of general and specific deterrence in affecting behavior. Specific deterrence is the "enforcement against a particular violator on *that* violator's future conduct, while general deterrence refers to effects of visible enforcement in the legal environment on *other* would-be violators who have yet to actually be the targets of enforcement, and hope never to be."

388. *See supra* notes 315–16 and accompanying text; *see also supra* note 325–26 and accompanying text.

389. *2018 Small Business Profile*, U.S. SMALL BUS. ADMIN. OFFICE OF ADVOCACY (2018), https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf.

2015.[390] Consequently, the U.S. economy cannot afford to have a fine so large that it pushes small businesses to bankruptcy.[391] Thus, the U.S. federal privacy law must find the delicate balance when setting its fines so that it acts as a specific deterrent, but does not drive out small business in America.

A proper solution would be to set a fine that is a percentage of the organization's revenue. The GDPR's fines in Article 83 are a percentage of an organization's revenues, but only if that fine would be greater than €10 or €20 million, depending on the violation. The United States can improve upon Article 83 of the GDPR by setting the fines for violations of a federal U.S. privacy law at a fixed percentage of an organization's revenues. By using a percentage of revenue approach rather than a massive fine like the GDPR, a U.S. privacy law can act as a specific deterrent to companies but will not drive them out of business. A percentage of revenue approach will achieve this purpose because the fine will then be a sliding scale depending on the size of the business that violated the U.S. federal privacy law.[392] Therefore, by setting fines as a percentage of an

---

390. *Id.*

391. *See Hearing on Protecting Consumer Privacy in the Era of Big Data Before the H. Comm. On Energy and Commerce and S. Comm. On Consumer Protection and Commerce*, 116th Cong. (2019) (statement by Roslyn Layton, Visiting Scholar, The American Enterprise Institute) ("To do business in the EU today, the average firm of 500 employees must spend about $3 million to comply with the GDPR. Thousands of US firms have decided it is not worthwhile and have exited. No longer visible in the EU are the *Chicago Tribune* and the hundreds of outlets from Tribune Publishing [. . .] Of course, $3 million, or even $300 million, is nothing for Google, Facebook, and Amazon (The Fortune 500 firms have reportedly earmarked $8 billion for GDPR upgrades.), but it would bankrupt many online enterprises in the US. Indeed, less than half of eligible firms are fully compliant with the GDPR; one-fifth say that full compliance is impossible." (footnotes omitted)).

392. For example, a 4% fine of Facebook's revenues will be a strong enough punishment to deter Facebook from violating the law. At the same time, a 4% fine of a small business' revenue will also be a strong enough punishment to deter that small business from violating the law, while also not driving the small

organization's revenues, a U.S. federal privacy law can both act as a specific deterrent to shape a business' future behavior, but not be so drastic that it drives small businesses out of the industry.

CONCLUSION

In today's digital age, data breaches have become commonplace. In 2017, there were a record high 1,579 data breaches,[393] with the most damaging data breach being the Equifax data breach in the summer of 2017.[394] Although the American legal system currently does not have enough protections for consumers in place, the Equifax data breach presents an opportunity to improve consumer protection in America. Accordingly, following the Equifax breach, lawmakers have already proposed legislation to improve consumer protection.[395]

However, this Comment argues that there are two distinct steps that can be made within the legal community to improve consumer protection. First, the Supreme Court can rule on Article III standing in a data breach case and clearly state that risk of future harm from a data breach constitutes an injury-in-fact under Article III.[396] This will allow victims of a data breach to have their day in court with a class action lawsuit and deter companies from failing to put into place proper cybersecurity protections for their customers' valuable personal information. Second, a federal privacy law will ensure that those affected by a data breach are properly notified of the breach in a timely manner.[397] A federal law with appropriate fines for noncompliance will

---

business to bankruptcy.

393. *See supra* note 42 at 3.

394. *See supra* Part III.

395. *See supra* note 370.

396. *See supra* Section V.A.

397. *See supra* Section V.B.

also act as a specific deterrent for companies to ensure that they comply with the law. This will ensure that victims of a breach are notified in a timely manner and allow them to make the appropriate accommodations to protect themselves from further harm.

Overall, cybersecurity is a complex and new area of the law. As Dwight Schrute said, identity theft is "not a joke" and it's time America took it seriously.[398] Data breaches pose a significant threat to consumers, affecting their personal and financial security. The severity of data breaches requires society and the law to adapt accordingly and ensure that consumers are protected. If the proper steps are taken, the American legal system can provide proper protection for its citizens.

Editor's Note: This Comment was selected from our 2017–18 Note & Comment competition. Simultaneous with its publishing, the Federal Trade Commission announced that it reached a settlement of approximately $700 million with Equifax in relation to the 2017 Equifax data breach. For more information regarding this settlement, see the Federal Trade Commission's statement here: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

398. *See supra* note 1 and accompanying text.