WAKE FOREST JOURNAL OF BUSINESS AND INTELLECTUAL PROPERTY LAW

VOLUME 18 SPRING 2018 NUMBER 3

COMMENT: CORPORATE LIABILITY FOR DATA BREACHES: WILL EQUIFAX VICTIMS HAVE A LEG TO STAND ON?

Emily Marcum†

I. INTRODUCTION 527

II. BACKGROUND 533

A. *CLAPPER V. AMNESTY INTERNATIONAL USA* 533

B. *SPOKEO, INC. V. ROBINS* 536

III. DISCUSSION 538

A. D.C. CIRCUIT FINDS THAT A DATA BREACH INCREASING RISK OF IDENTITY THEFT IS ENOUGH TO ESTABLISH ARTICLE III STANDING 539

B. THE SIXTH, SEVENTH, AND ELEVENTH CIRCUITS FIND THAT AN INCREASED RISK OF FUTURE HARM IS SUFFICIENT TO ESTABLISH ARTICLE III STANDING AT THE PLEADING STAGE 542

1. Galaria v. Nationwide Mutual Insurance Company 542

2. Lewert v. P.F. Chang's China Bistro, Inc. 545

3. Resnick v. AvMed, Inc. 547

C. THE SECOND AND FOURTH CIRCUITS FIND THAT AN INCREASED RISK OF FUTURE HARM IS INSUFFICIENT TO ESTABLISH ARTICLE III STANDING 548

1. Whalen v. Michaels Stores, Inc. 548

2. Beck v. McDonald 550

† © 2018 J.D. 2018, Wake Forest University School of Law; B.A. 2015, University of South Carolina. First and foremost, I would like to thank my parents, Don and Margaret Marcum, for their endless love, support, and encouragement. Without you, I would not be the woman I am today. I am forever grateful and credit every one of my successes to the two of you. Second, I would like to thank all of the wonderful professors I have had at Wake over the past three years. Your wisdom, patience, dedication, and desire to make the world a better place has been beyond inspirational. Finally, I would like to thank the entire *Wake Forest Journal of Business and Intellectual Property Law* staff for your hard work in editing this article.

D. COURTS SHOULD FIND THAT EQUIFAX VICTIMS MEET ALL THREE ELEMENTS REQUIRED TO ESTABLISH ARTICLE III STANDING 551

IV. CONCLUSION 554

I. INTRODUCTION

News of corporate data breaches littering headlines have become as ubiquitous as those about President Trump's visits to Mar-a-Lago.[1] Both occur frequently, are unsurprising, and are costing Americans a great deal of money.[2] But what is being done to change this narrative? It is likely that at some point nearly every individual has encountered an employer, a government official, a tech-savvy cousin, an online retailer, or an educational institution's IT department, who stresses the importance of cybersecurity or password protection.[3] The likely response from the individual is a smile, nod, and promise to stop using the password created ten years ago for an AOL account that merely combined a name and birthday. A password so simple that it does not even stump a computer illiterate grandmother. Unfortunately, it is time to realize that the individuals stressing the importance of password diversification and cybersecurity are not just lecturing for fun, and the data breach headlines that seem to greet us daily must be taken seriously.[4]

Identity theft and fraud have recently reached unprecedented heights. In 2016, 15.4 million consumers in the United States were victims of identity theft or fraud; a number up sixteen percent from 2015.[5] Identity thieves were able to steal a total amount of sixteen

---

[1] *See, e.g.*, Associated Press, *Here's How Much It Costs Taxpayers for Donald Trump to Stay at His Weekend Getaways*, FORTUNE (May 8, 2017), http://fortune.com/2017/05/08/donald-trump-travel-security-costs/ (providing an example of a recent headline regarding President Trump's trips to Mar-a-Lago).

[2] *See id.*

[3] *See* Dr. Detlev Gabel et al., *Cyber Risk: Why Cyber Security is Important*, WHITE & CASE (July 1, 2015), https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important (citing the World Economic Forum's statistic that ninety percent of companies worldwide are insufficiently prepared to protect themselves against cyber-attacks, at a cost of $400 billion annually); *see also* Sharon Profis, *The Guide to Password Security (And Why you Should Care)*, CNET, (Jan. 1, 2016, 7:20 AM), https://www.cnet.com/how-to/the-guide-to-password-security-and-why-you-should-care (listing several factors to consider when creating a password to maximize personal password security).

[4] *See, e.g.*, *Equifax Under Pressure After Data Breach Update*, BBC (Feb. 12, 2018), http://www.bbc.com/news/technology-43033202; Sasha Lekach, *FedEx Customer Information Exposed in Data Breach*, YAHOO!: NEWS (Feb. 15, 2018), https://uk.news.yahoo.com/fedex-customer-information-exposed-data-205710707.html; Mathew J. Schwartz, *US Data Breaches Hit All-Time High*, INFO. SECURITY MED. GROUP (Feb. 1, 2018), https://www.bankinfosecurity.com/us-data-breaches-hit-all-time-high-a-10622.

[5] Kelli B. Grant, *Identity Theft, Fraud Cost Consumers More than $16 Billion*, CNBC (Feb. 1, 2017, 9:11 AM), https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

continued . . .

billion dollars.[6] If the monetary threat alone is not enough to incentivize individuals to take cybersecurity seriously, perhaps the inconvenience of spending hours on hold with customer service representatives while being forced to listen to classical tunes and smooth jazz will be. Fortunately, there are steps that individuals can and should take to better protect themselves from identity thieves.[7] Unfortunately, there are some instances of corporate data breaches where even a 10,000-character password has not provided sufficient protection because the breach was a consequence of a flaw in the corporation's software,[8] the most recent example being Equifax.

Equifax, one of the three major consumer credit reporting agencies in the United States, discovered it was hacked on July 29, 2017.[9] In March 2017, Equifax discovered a technological flaw in its software that led to its demise and the hackers' success.[10] However, Equifax failed to take action in patching the deficiency.[11] As a result, the Equifax hacker(s) was able to steal the personal information of 147.9 million consumers.[12] Although the Equifax breach is not as large as the 2013 Yahoo! breach, which affected the entirety of its three billion accounts,[13] or as embarrassing as the 2015 breach of the original "extramarital dating site" known as Ashley Madison,[14] there are certain

[6] *Id.*

[7] *See generally How to Protect Yourself from Identity Theft*, CONSUMER REPS. (July 2010), https://www.consumerreports.org/cro/2010/07/protect-your-identity/index.htm (discussing steps that consumers can take to protect themselves from identity fraud which include: freezing accounts, securing internet-connected devices, and opting out of receiving unsolicited credit card offers that thieves use in identity theft).

[8] Ken Sweet & Michael Liedtke, *Equifax Traced the Source of its Massive Hack to a Preventable Software Flaw*, BUS. INSIDER (Sept. 14, 2017, 7:55 PM), http://www.businessinsider.com/how-did-equifax-get-hacked-2017-9.

[9] Jade Scipioni, *Equifax Hack: A Timeline of Events*, FOX BUS. (Oct. 17, 2017), http://www.foxbusiness.com/features/2017/09/14/equifax-hack-timeline-events.html.

[10] *See* Sweet & Liedtke, *supra* note 8.

[11] *Id.*

[12] *See* Michael R. Bartosik & Steven M. Packer, *Still Worried About the Equifax Breach? So Are 145 Million Others*, LEXOLOGY (Oct. 19, 2017), https://www.lexology.com/library/detail.aspx?g=73e56199-c875-4f28-9d11-7a4f7436430c; Nick Clements, *Equifax's Enormous Data Breach Just Got Even Bigger*, FORBES (Mar. 5, 2018), https://www.forbes.com/sites/nickclements/2018/03/05/equifaxs-enormous-data-breach-just-got-even-bigger/#3198c54d53bc (finding an additional 2.4 million Americans were impacted by the data breach).

[13] Lily H. Newman, *Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts*, WIRED (Oct. 3, 2017, 7:29 PM), https://www.wired.com/story/yahoo-breach-three-billion-accounts/.

[14] Alex Hern, *Hacked Dating Site Ashley Madison Agrees to Pay $11m to US-Based Users*, GUARDIAN (July 17, 2017, 11:26 PM),

continued . . .

elements regarding the Equifax breach that make it more malevolent than any of its predecessors' breaches.

First, unlike the Yahoo! or Ashley Madison breaches, individuals did not need to create an account or use Equifax's services for Equifax to receive the individual's personal and financial information.[15] Equifax may receive an individual's information regardless of whether one consented to its collection or had a business relationship with Equifax.[16] This is because Equifax is a credit reporting agency, and a large-scale data aggregator.[17] Not only does Equifax collect the data provided to it, but it also collects and purchases data from third parties.[18] These third parties include banks, mortgage brokers, credit card companies, and any other business that extends credit.[19] Thus, if an individual ever borrowed money or extended credit, then Equifax has likely received that individual's most sensitive personal information from a third party.[20] This sensitive personal information may include, but is not limited to, date of birth, address, Social Security number, credit score, financial history, and driver's license number.[21] This kind of information makes it possible for those with ill motives to cause a lifetime of headaches by impersonating individuals to banks, credit card companies, the Internal Revenue Service, insurance companies, and other businesses susceptible to fraud.[22] In addition, most of the information stolen in the Equifax breach is incredibly difficult for consumers to change.[23] The nature of this stolen information increases

https://www.theguardian.com/technology/2017/jul/17/hacked-dating-site-ashley-madison-parent-company-ruby-life-inc-pay-11m-dollars-us-based-users.

[15] *See* Bruce Schneier, *Don't Waste Your Breath to Equifax About Data Breach*, CNN (Sept. 11, 2017, 6:23 PM), http://www.cnn.com/2017/09/11/opinions/dont-complain-to-equifax-demand-government-act-opinion-schneier/index.html; *see also* Jeff Pollard & Joseph Blankenship, *Equifax Does More Than Credit Scores*, FORBES (Sept. 8, 2017, 6:06 PM), https://www.forbes.com/sites/forrester/2017/09/08/equifax-does-more-than-credit-scores/#6fee659319d8 ("Equifax collects information about you. You may not know it does, but it does. Even if you aren't in the population of breached users, they know you. You don't know what they know about you, and you have no way to find out in normal circumstances.").

[16] Pollard & Blankenship, *supra* note 15.

[17] *Id.*

[18] *See id.*

[19] Brenda R. Sharton & David S. Kantrowitz, *Equifax and Why It's So Hard to Sue a Company for Losing Your Personal Information*, HARV. BUS. REV. (Sept. 22, 2017), https://hbr.org/2017/09/equifax-and-why-its-so-hard-to-sue-a-company-for-losing-your-personal-information.

[20] *See id.*

[21] Schneier, *supra* note 15.

[22] *See id.*

[23] *See id.* (explaining that hackers are interested in accessing permanent and semi-permanent information like individuals' full names, Social Security numbers,

continued . . .

the likelihood that consumers' identities will be stolen in the future. Consumers looking to sue regarding this future harm will likely face difficulties in establishing Article III standing.

Another reason the Equifax breach is unique is because the three consumer credit bureaus are normally the points of contact for consumers after a consumer realizes their identity has been stolen.[24] This stems from the fact that consumer credit bureaus provide services such as credit monitoring and identity theft protection, which are typically utilized by the victims of identity fraud.[25] This means that the 147.9 million consumers that were victims of the Equifax hack are left in the awkward predicament of trusting the company whose very negligence led to their misfortune.[26] Instead of purchasing identity theft protection and credit monitoring services from Equifax, outraged and disappointed consumers likely searched for an alternative identity theft protection service like LifeLock.[27] What many consumers do not realize is that a majority of these alternative services have contracts with one of the three major credit reporting agencies.[28] In this arrangement, the credit reporting agencies provide the alternate services with certain credit products and services that the alternate services then turn around and use in their own identity theft protection services.[29]

One example of this arrangement is between LifeLock and Equifax.[30] LifeLock has exploited Equifax's massive blunder by increasing advertising, and targeting Equifax victims.[31] As a result, LifeLock's enrollment is ten times greater than its enrollment was before the breach.[32] However, many consumers do not realize that by purchasing services from LifeLock, they are actually signing up for services provided by Equifax.[33] In addition, if a consumer would like to freeze their credit so identity thieves cannot open up accounts in that consumer's name and ruin their credit score, the consumer is required

---

birth dates, addresses, and driver's license numbers).

[24] *See* Sharton & Kantrowitz, *supra* note 19.

[25] *See id.*

[26] *Id.*; Clements, *supra* note 12.

[27] *See* Michael Hiltzik, *LifeLock Offers to Protect You From the Equifax Breach—by Selling You Services Provided by Equifax*, L.A. TIMES (Sept. 18, 2017, 1:15 PM), http://www.latimes.com/business/hiltzik/la-fi-hiltzik-lifelock-equifax-20170918-story.html. LifeLock is an American company that specializes in identity theft protection services. *Id.*

[28] *See id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

continued . . .

to pay Equifax a monthly fee.[34] After breach victims expressed their absolute outrage in paying Equifax for a service that was only made necessary because of Equifax's own negligence, Equifax begrudgingly agreed to waive the freeze fee through November 21, 2017.[35]

Nonetheless, Equifax is profiting, or will eventually profit, off its own negligence which caused the identity theft victims' misfortune.[36] As if this has not caused enough outrage, Equifax's negligence went even further when it took forty-one days after learning of the breach to notify consumers.[37] During that forty-one days, three of Equifax's top executives sold over two million dollars of their company stock.[38]

There is a lack of accountability in the industry, primarily because there are only three credit reporting agencies. The three agencies, Equifax, Experian, and TransUnion, have a virtual monopoly on the credit reporting industry.[39] These three agencies are used by 90 percent of lenders, leaving consumer-borrowers with very few alternative choices.[40]

"Credit reporting agencies are grease in the great American credit engine. Lenders need them, and borrowers need lenders. If Equifax were to go away, it would merely make TransUnion and Experian more powerful, but probably no less vulnerable to hacking themselves."[41] These three companies are almost too big to fail, and therefore, maintain a sense of security because of their size and control over the credit reporting industry.[42] Their indifference is founded upon the fact that

---

[34] Sarah O'Brien, *Here's What it Costs to Freeze Your Credit After Equifax Breach*, CNBC (Sept. 15, 2017, 8:50 AM), https://www.cnbc.com/2017/09/15/heres-what-it-costs-to-freeze-your-credit-after-equifax-breach.html.

[35] Ron Lieber, *Equifax, Bowing to Public Pressure, Drops Credit-Freeze Fees*, N.Y. TIMES (Sept. 12, 2017), https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html.

[36] Jen Wieczner, *How Equifax is 'Making Millions of Dollars Off its Own Screwup'*, FORTUNE (Oct. 4, 2017), http://fortune.com/2017/10/04/equifax-breach-elizabeth-warren/.

[37] Scipioni, *supra* note 9.

[38] *Id.*

[39] David Dayen, *Break Up the Credit-Reporting Racket*, THE NEW REPUBLIC (Sept. 12, 2017), https://newrepublic.com/article/144780/break-credit-reporting-racket.

[40] *Id.*

[41] Editorial Board, *Equifax is Too Big to Fail, Not Too Big to Hold Accountable*, ST. LOUIS POST DISPATCH (Sept. 12, 2017), http://www.stltoday.com/opinion/editorial/editorial-equifax-is-too-big-to-fail-not-too-big/article_23fe5ec8-bff1-5aae-9085-e0fb714408ea.html.

[42] Thomson Gale, *Credit Bureaus*, ENCYCLOPEDIA, https://www.encyclopedia.com/social-sciences-and-law/economics-business-and-labor/businesses-and-occupations/credit-bureau (last visited Mar. 19, 2018) (discussing that most of the over 1000 consumer credit bureaus in the United States

continued . . .

those individuals who utilize credit reporting agencies are not the customer; they are the product.[43] Equifax's real customers are the employers, businesses, lenders, and landlords looking to purchase information on individuals.[44] As a result, there is a clear lack of accountability and an indifference when it comes to consumers who are essentially the credit reporting agencies' product.[45] Thus, regardless of whether it be legal recourse or government regulation, action must be taken.[46]

Consumers looking to sue for an increased risk of future identity theft will likely run into one very large obstacle: establishing Article III standing.[47] Part II of this Comment will first discuss the basic elements required to establish Article III standing. Part II will then describe two landmark Supreme Court cases that apply these elements to scenarios involving a risk of future harm. Part III of this Comment will analyze the string of recent cases that define a widening circuit split involving the issue of whether an increased risk of future harm satisfies the first Article III element of injury-in-fact. Additionally, Part III will analyze the facts of the Equifax breach, comparing them to the facts of other circuit opinions, and discuss the likelihood of victims successfully establishing Article III standing. Lastly, Part IV will conclude with potential solutions to establishing standing to sue after data breaches, and propose ways to hold corporations more accountable, so that the negligent protection of consumers' private information is made intolerable.

---

are either owned or under contract with the three major credit reporting agencies and each of the three major credit reporting agencies maintain over 190 million credit files).

[43] Schneier, *supra* note 15.

[44] *Id.*

[45] *See generally* Frank Pasquale, *The Dark Market for Personal Data*, N.Y. TIMES (Oct. 16, 2014), https://www.nytimes.com/2014/10/17/opinion/the-dark-market-for-personal-data.html (explaining that the market for personal information encourages the pursuit of reaching a threshold percentage of information rather than delivering accurate information, and it does so at the expense of individuals and their reputations).

[46] *See* Editorial Board, supra note 41. *See also* Pasquale, *supra* note 45 (specifying the various laws and regulations the article's author believes society should implement).

[47] *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (explaining that in order to have standing, litigants must show that their lawsuit is seeking redress for legal wrong, and federal courts will not overstep the bounds of their judicial role by hearing the case if there is no standing).

continued . . .

II. BACKGROUND

Before a plaintiff can sue Equifax for an increased risk of future identity theft caused by its failure to safeguard consumers' personal information, the plaintiff must first establish standing.[48] Although the Constitution does not explicitly require that a plaintiff possess standing to file a suit in federal court, the Supreme Court has inferred a standing requirement from the language of Article III of the United States Constitution.[49] Article III limits federal courts' jurisdiction to "cases and controversies."[50] Therefore, the standing requirement ensures that federal courts have subject matter jurisdiction, and "do not exceed their authority as it has been traditionally understood."[51] To successfully establish Article III standing, a plaintiff has the burden of proving three elements: (1) the plaintiff must have suffered an "injury-in-fact" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"; (2) the injury is "fairly traceable to the challenged action of the defendant"; and (3) the injury is "likely" to be "redressed by a favorable decision."[52] If a plaintiff fails to meet all of these elements, a federal court must dismiss the case without deciding the merits.[53]

A. *Clapper v. Amnesty International USA*

The leading case on claims of standing based on risk of future harm is *Clapper v. Amnesty International USA*.[54] In *Clapper*, the plaintiffs challenged § 1881 of the Foreign Intelligence Surveillance Act ("FISA"), which permitted the United States government to spy on the

[48] *See* Raines v. Byrd, 521 U.S. 811, 818 (1997) ("One element of the case-or-controversy requirement is that appellees, based on their complaint, must establish that they have standing to sue.").

[49] Section 2 of Article III provides: "The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;–to all Cases affecting Ambassadors, other public Ministers and Consuls;–to all Cases of admiralty and maritime Jurisdiction;–to Controversies to which the United States shall be a Party;–to Controversies between two or more States;–between a State and Citizens of another State;-between Citizens of different States;–between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects." U.S. CONST. art. III, § 2.

[50] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

[51] *Spokeo*, 136 S. Ct. at 1547.

[52] Lujan v. Defs. of Wildlife, 504 U.S. 555, 555–61 (1992).

[53] Bradford C. Mank, *Clapper v. Amnesty International: Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 219 (2014).

[54] *Clapper,* 568 U.S. at 398.

continued . . .

communications of foreign nationals outside the United States.[55] Plaintiffs alleged that although they were not foreign nationals, there was an "objectively reasonable likelihood" the government would intercept their communications with overseas contacts..[56] The plaintiffs in *Clapper* were a diverse group of "attorneys and human rights, labor, legal, and media organizations whose work allegedly require[d] them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located [outside the United States]."[57] The plaintiffs asserted their belief that some of the foreign nationals with whom they communicate were "likely targets of government surveillance under § 1881a" because the contacts were "located in geographic areas that [were] a special focus of the Government's counterterrorism or diplomatic efforts" and because some of these contacts were people that the Government "believe[d] to be associated with terrorist organizations."[58] The plaintiffs claimed that the § 1881a provision of FISA interfered with their "ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[59] As a result, plaintiffs alleged that they avoided "engaging in certain telephone and e-mail conversations" which would eventually force them to incur expenses to "travel abroad in order to have in-person conversations."[60]

The United States Supreme Court majority used the "certainly impending" standard in deciding whether the plaintiffs met Article III standing.[61] The Court declared that "'threatened injury must be *certainly impending* to constitute injury-in-fact,' . . . 'allegations of *possible* future injury' are not sufficient."[62] However, in footnote five, the Court also noted that it had previously "found standing based on a 'substantial risk' that the harm will occur."[63] The "substantial risk"

[55] *Id.* at 407.
[56] *Id.*
[57] *Id.* at 406 (alteration in original).
[58] *Id.* (alteration in original).
[59] *Id.*
[60] *Id.* at 406–07.
[61] *Id.* at 401.
[62] *Id.* at 410 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).
[63] *Id.* at 414 n.5 ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm. But to the extent that the 'substantial risk' standard is relevant and is distinct from the "clearly impending" requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here.").

continued . . .

standard mentioned in footnote five appears to be slightly more lenient than the "certainly impending" standard.[64] Unlike the "certainly impending" standard, the "substantial risk" standard does not require a plaintiff to demonstrate that they are certain that the harms identified will come about, but rather only need to demonstrate that there is a "substantial risk" the harm will occur.[65] However, the Court found that the plaintiffs failed to establish an injury-in-fact under both the "certainly impending" test and the "substantial risk test" because the injury the plaintiffs feared was too speculative and "relies on a highly attenuated chain of possibilities," none of which had been alleged to have occurred at the time of the lawsuit.[66]

Since *Clapper* discussed the two aforementioned standards, courts have been split as to whether an increased risk of future harm is enough to establish the first element of "injury-in-fact."[67] *Clapper* suggested that a "highly speculative fear" of injury that was not "certainly impending" failed to establish an injury-in-fact.[68] This holding has made it difficult for victims of corporate data breaches to hold corporations liable for the risk of future harm they suffer from having their information stolen.[69] The *Clapper* holding implies that a hacker has to steal a consumer's identity and actually participate in fraudulent activity in order for the consumer to meet the Article III injury-in-fact requirement.[70]

---

[64] *Id.*

[65] *Id.*

[66] *Id.* at 410–11.

[67] *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 692 (D.C. Cir. 2017) (holding that the plaintiffs had standing to bring data breach claims when the defendant had already accessed personal information, and it was thus plausible to infer that the defendant had "both the intent and ability to use the data for ill"); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385–386 (6th Cir. 2016) (holding that the plaintiffs had standing to bring data breach claims when the breached database contained personal information such as "names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers"). *But see* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (holding that the plaintiff did not have standing to bring a claim of credit card fraud against the store because she did not allege "how she [could] plausibly face a threat of future fraud" if her stolen credit card was promptly canceled and no other personally identifying information was alleged to have been stolen).

[68] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409–10 (2013).

[69] *See generally* Thomas Martecchini, Note, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After Clapper v. Amnesty International USA,* 114 MICH. L. REV. 1471 (2016) (discussing the difficulty of establishing standing based on future harm after *Clapper*).

[70] *Id.*

continued . . .

B. *Spokeo, Inc. v. Robins*

Three years after the *Clapper* decision caused a circuit split regarding whether a risk of future harm could constitute an injury-in-fact, the Supreme Court heard *Spokeo Inc. v. Robins*, an appeal out of the Ninth Circuit.[71] In hearing this case, the Supreme Court finally had the opportunity to declare whether a risk of future harm was enough to constitute an injury-in-fact for purposes of establishing Article III standing. To the dismay of many, the Supreme Court focused on the Ninth Circuit's "inadequate standing" analysis and did not explicitly address whether increased risk of future harm constitutes an injury-in-fact.[72]

Robins, the plaintiff in *Spokeo*, filed a class action lawsuit against Spokeo alleging that the company willfully failed to comply with the Fair Credit Reporting Act ("FCRA") after posting inaccurate information about him online.[73] Spokeo operates as a "people search engine" that provides personal information about individuals to a variety of users, including employers researching prospective employees.[74] After a user submits an inquiry online, Spokeo searches a multitude of databases, and then collects and provides that information to the user.[75] This information includes an individual's address, phone number, marital status, age, occupation, hobbies, financial history, shopping habits, and even their musical preferences.[76] Robins asserted that the profile Spokeo created without his consent stated that he was married, had children, was in his fifties, had a job, was economically affluent, and held a graduate degree.[77] All of these things were false.[78] Robins claimed that the inaccurate information published by Spokeo caused him to "suffer actual harm to his employment prospects" because it made him appear overqualified, expectant of a higher salary, and unlikely to relocate because of family obligations.[79]

The Ninth Circuit held that Robins adequately alleged an injury-in-fact, but the Supreme Court found that the court of appeals failed to analyze whether the injury was concrete in addition to being particularized.[80] To establish an injury-in-fact, a plaintiff has the

[71] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1543 (2016).
[72] *Id.*
[73] *Id.*
[74] *Id.* at 1543, 1546.
[75] *Id.*
[76] *Id.* at 1546.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 1554.
[80] *Id.* at 1545.

continued . . .

burden of showing that they have suffered an "invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[81] The Supreme Court explained that in order for an injury to be particularized, it must "affect the plaintiff in a personal and individual way."[82] The Supreme Court determined that, while particularization is necessary to establish an injury-in-fact, particularization alone it is not sufficient.[83] An injury-in-fact must also be "concrete."[84] For an injury to be considered "concrete," it must actually exist.[85] Further, the Supreme Court clarified that an injury does not have to be tangible in order to be concrete.[86] In particular, the Supreme Court noted that:

> "Concrete" is not . . . synonymous with "tangible." Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete. In determining whether an intangible harm constitutes injury-in-fact, both history and the judgment of Congress play important roles.[87]

Although the Supreme Court clarified that the alleged harm does not have to be tangible to be concrete and particularized, it failed to explicitly identify whether an increased risk of future harm is enough to satisfy the element of imminence.[88] Additionally, the Supreme Court said that Congress cannot automatically conclude that an intangible harm satisfies injury-in-fact where a statute grants a person a statutory right and appears to authorize that person to sue to vindicate that right.[89] Instead, a statutory right to sue is insufficient in establishing Article III standing, unless the violation of a statutory right is combined with a concrete injury.[90] However, even in cases where the risk of real future harm is difficult to prove or hard to measure, the injury may still be concrete.[91]

Ultimately, the Supreme Court vacated the Ninth Circuit's decision and remanded the case, instructing the Ninth Circuit to analyze both

[81] Lujan v. Defs. of Wildlife, 112 S. Ct. 2130, 2136 (1992).
[82] *Spokeo*, 136 S. Ct. at 1548.
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.* at 1549.
[87] *Id.* (citation omitted).
[88] *Id.* at 1550.
[89] *Id.* at 1549.
[90] *Id.* at 1547–48.
[91] *See id.* at 1549.

continued . . .

concreteness and particularization to determine whether the plaintiff satisfies the first element of injury-in-fact.[92] Although the Supreme Court left lower courts, consumers, and businesses wondering whether a data breach is imminent enough for consumers to sue the party who failed to protect their data when the breach results in an increased risk of identity theft by a third party, the Court did provide the above clarifications with respect to analyzing particularization and concreteness.[93] Unfortunately, *Spokeo* did nothing to resolve the circuit split resulting from *Clapper*. Circuits remain split on whether the risk of future harm is imminent enough to establish Article III standing, and now they are wrestling with exactly how *Spokeo* applies to allegations of an increased risk of identity theft following a data breach.[94]

III. DISCUSSION

The Supreme Court's failure to utilize its opportunity in *Spokeo* to explicitly address whether a claim of increased risk of future harm is concrete and imminent enough to constitute an injury-in-fact caused the circuit split following *Clapper* to widen even further.[95] The D.C. Circuit's recent ruling, in *Attias v. CareFirst*, "amplifies the circuit split by strengthening the hand of potential class action litigants, and it may signal a potential turning of the tide on the issue of standing when the data breach involves intentional hacking."[96] The D.C., Sixth, Seventh, and Eleventh Circuits all agree that an increased risk of future identity theft constitutes an injury-in-fact, satisfying at least the first element of Article III standing.[97] Conversely, the Second and Fourth Circuits have found that a mere increased risk of identity theft or future harm is neither concrete nor imminent enough to constitute the injury-in-fact element required for Article III standing.[98] The following sections will explore

[92] *Id.* at 1545.

[93] *See generally id.* (vacating and remanding to the Ninth Circuit because of a failure to adequately analyze standing). The Supreme Court did not address Respondent's concerns over Spokeo's failure to adhere to the FCRA. *See id.*

[94] *Id.* at 1549.

[95] Edward R. McNicholas & Grady Nye, *D.C. Circuit Widens the Split on Standing in Data Breach Cases After Spokeo*, LEXOLOGY (Aug. 8, 2017), https://www.lexology.com/library/detail.aspx?g=7335a949-2364-4f44-9c2a-74939d5ea1da.

[96] *Id.*

[97] *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 970 (7th Cir. 2016); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 391–92 (6th Cir. 2016); Resnick v. AvMed, Inc., 693 F.3d 1317, 1327–28 (11th Cir. 2012).

[98] *See generally* Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017) ("[T]o establish Article III standing, a future injury must be 'certainly impending,' rather than simply speculative. [A] 'theory of standing which relies on

continued . . .

in detail a handful of the circuit opinions that took place over the past six years. Some of these opinions range from before *Clapper* and *Spokeo* and others are as recent as last year. Finally, this section will use this case law to determine the likelihood of Equifax victims successfully establishing Article III standing.

A. D.C. Circuit Finds That a Data Breach Increasing Risk of Identity Theft is Enough to Establish Article III Standing

In the most recent case following *Spokeo*, the D.C. Circuit held that a data breach that increases a plaintiff's risk of identity theft is enough to establish an injury-in-fact for purposes of Article III standing.[99] In June 2014, CareFirst, a health insurance company, "suffered a cyberattack in which its customers' personal information" was stolen after an unknown intruder breached twenty-two CareFirst computers.[100] CareFirst did not discover the breach until April 2015, and it failed to notify its customers until over a month later.[101] This breach included sensitive and personally identifiable customer information, such as legal names, birthdates, email addresses, health insurance subscriber identification numbers, Social Security numbers, and credit card information.[102] Plaintiffs alleged that CareFirst's failure to properly encrypt the stored data caused the cyberattack and caused the plaintiffs to experience a heightened risk of identity theft.[103] The affected customers brought a class action lawsuit that raised eleven different state law causes of action, including breach of contract, negligence, and violation of various state consumer protection statutes.[104]

The district court dismissed the suit for lack of standing after concluding that the injury was too speculative because the plaintiffs failed to allege a present injury or a high enough likelihood of future

---

a highly attenuated chain of possibilities does not satisfy the requirement that threatened injury must be certainly impending.'"); *see also* Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017) (finding "*Clapper*'s rejection of the Second Circuit's attempt to import an 'objectively reasonable likelihood' standard into Article III standing to express the common-sense notion that a threatened event can be 'reasonably likely' to occur but still be insufficiently 'imminent' to constitute an injury-in-fact").

[99] *Attias*, 865 F.3d at 629.

[100] *Id.* at 622–23.

[101] *Id.* at 623.

[102] *Id.*

[103] *See id.*

[104] *Id.* ("The plaintiffs sought to certify a class consisting of all CareFirst customers residing in the District of Columbia, Maryland, and Virginia whose personal information had been hacked.").

continued . . .

injury.[105] The district court mistakenly based this conclusion on its misunderstanding that the stolen information did not include the plaintiffs' Social Security and credit card numbers.[106] Without stolen Social Security numbers and credit card numbers, the threat of identity theft was not actual or imminent; therefore, it could not satisfy Article III's first element of injury-in-fact.[107] However, the district court failed to realize that Social Security and credit card numbers were included under the plaintiffs' definitions for personal identification information ("PII"), personal health information ("PHI"), and electronic personal health information ("ePHI").[108] Therefore, the plaintiffs' complaint adequately alleged that the compromised data did include their Social Security numbers and credit card numbers.[109] Because of its misunderstanding, the district court wrongly dismissed the case and the plaintiffs appealed.[110] On appeal, the D.C. Circuit found that the plaintiffs indeed plausibly alleged a risk of future injury substantial enough to meet all three standing elements required under Article III.[111]

In regard to Article III's first element of injury-in-fact, the court stated that "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."[112] Additionally, the D.C. Circuit found it was plausible to infer that the hacker had both "the intent and the ability to use the data for ill."[113] Ultimately, the D.C. Circuit Court concluded that the sensitive nature of the information stolen automatically created a substantial risk of harm, satisfying the injury-in-fact requirement.[114] Further, the D.C. Circuit determined that the "substantial risk" standard, first mentioned in footnote five of the *Clapper* opinion, would be the key test for evaluating future data breach cases.[115] "No long sequence of uncertain

---

[105] *See id.*

[106] *See id.*

[107] *See id.* (explaining that although the personal information could be accessed, there had been no injury, i.e. credit fraud or identity theft, at the time of the complaint and the only reported injury was a breach of the security network).

[108] *Id.* at 627.

[109] *Id.* at 628.

[110] *Id.* at 623.

[111] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

[112] *Attias*, 865 F.3d at 627.

[113] *Id.* at 628. The Seventh Circuit drew a similar inference in *Remijas v. Neiman Marcus Group*, where it stated, "[w]hy else would hackers break into a 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." Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

[114] *Attias*, 865 F.3d at 629.

[115] *See id.* at 622, 626, 628–29 (recognizing *Clapper* as the leading case on

continued . . .

contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."[116]

The D.C. Circuit took it a step further and said that even if the plaintiffs had not alleged that their Social Security and credit card numbers had been stolen, the mere fact that health insurance subscriber identification numbers were stolen was enough for the court to find that the plaintiffs satisfied the injury-in-fact element because of the threat of "medical identity theft."[117] The court noted that:

> "Medical identity theft" [is where] a fraudster impersonates the victim and obtains medical services in her name. That sort of fraud leads to "inaccurate entries in [victims'] medical records" and "can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs." These portions of the complaint would make up, at the very least, 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.[118]

In regard to the second element of Article III standing, the D.C. Circuit confronted CareFirst's defense that the plaintiffs' injury was "fairly traceable" only to the data thief.[119] Although it is true that the hacker would be the most immediate cause of the plaintiffs' injuries, CareFirst's failure to secure its customers' sensitive data was only one step removed in the causal chain, and therefore the injury was also "fairly traceable" to CareFirst.[120] The court reasoned that: "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires

---

claims of standing based on risk of future injury and applying the *Clapper* "substantial risk" standard to a data breach case). *See generally Clapper*, 568 U.S. at 414 n.5 ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. . . . In some instances, we have found standing based on "substantial risk" that the harm will occur. In addition, plaintiffs bear the burden of pleading and proving concrete facts showing that the defendant's actual action has caused the substantial risk of harm.").

[116] *Attias*, 865 F.3d at 629 (explaining the corrective effect of the new "substantial risk" standard).

[117] *Id.* at 628.

[118] *Id.* (alteration in original).

[119] *Id.* at 629.

[120] *Id.*

continued . . .

only that those injuries be 'fairly traceable' to the defendant."[121]

Finally, the D.C. Circuit found that the plaintiffs satisfied the third element of Article III standing because their injury would "likely be redressed by a favorable judicial decision."[122] The Supreme Court in *Clapper* asserted that where there is a "substantial risk" that a harm will occur, the threat of this risk may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.[123] Due to this effect, courts can award damages that allow a plaintiff to recoup these reasonably incurred expenses.[124] Here, the plaintiffs in *Attias* alleged that they incurred the costs of "responding to the data breach, . . . acquiring identity theft protection and monitoring, . . . conducting a damage assessment, [and] mitigation . . . ."[125] These costs coupled with the plaintiffs' substantial risk of identity theft, "creates the potential for them to be made whole by monetary damages," which is enough to satisfy the redressability requirement.[126] Consequently, the D.C. Circuit reversed the district court's order that dismissed the case for lack of standing.[127]

B. The Sixth, Seventh, and Eleventh Circuits Find That an Increased Risk of Future Harm is Sufficient to Establish Article III Standing at the Pleading Stage

1. Galaria v. Nationwide Mutual Insurance Company

In addition to the D.C. Circuit's *Attias* holding, the Sixth, Seventh, and Eleventh Circuits have also held that an increased risk of future harm is sufficient to support standing. Six months after the Supreme Court's decision (or lack thereof) in *Spokeo*, the Sixth Circuit heard *Galaria v. Nationwide Mutual Insurance Company*, where it found that plaintiffs Mohammad Galaria and Anthony Hancox successfully established Article III standing for their putative class action.[128] On October 3, 2012, hackers broke into Nationwide's computer network and stole the sensitive, personal information of approximately 1.1 million Nationwide customers.[129]

---

[121] *Id.*

[122] *Id.*

[123] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

[124] *Attias*, 865 F.3d at 629.

[125] *Id.* (alteration in original).

[126] *Id.* (explaining that the redressability requirement may be satisfied when the mitigation costs are combined with a potential for future harm that could "qualify as an injury-in-fact").

[127] *Id.* at 630.

[128] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 391 (6th Cir. 2016).

[129] *Id.* at 386.

continued . . .

The plaintiffs claimed that Nationwide, an insurance and financial-services company, was negligent because it failed to "establish and/or implement appropriate administrative, technical, and/or physical safeguards to ensure the security and confidentiality of plaintiff's and other Class Members' [sensitive personal information] . . . ."[130] The stolen information included names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers.[131] After Nationwide learned of the breach, it advised all of its customers to take steps to prevent and mitigate the misuse of the stolen data.[132] The company encouraged its customers to enroll in credit monitoring and an identity theft protection service,[133] and it agreed to pay for a year of credit monitoring services and offered to protect customers against up to one million dollars of identity fraud.[134] Additionally, Nationwide suggested that customers purchase fraud alert and pay for a security freeze to be placed on their credit.[135]

The plaintiffs alleged that the Nationwide data breach created an "imminent, immediate and continuing increased risk" of fraud and identity theft.[136] They further alleged that this risk was beyond speculative allegations of "possible future injury" or "objectively reasonable likelihood" of injury that the Supreme Court has previously found to be insufficient.[137] Plaintiffs alleged that there is an illicit international market for stolen data, which is used to obtain identification, government benefits, employment, housing, medical services, financial services, and credit and debit cards.[138] As a result, identity theft victims must forever be vigilant in monitoring not only their finances, but also their insurance and even their personal records to ensure there are no criminal charges in their name.[139] In order to redress the aforementioned risk, the plaintiffs sought damages for the increased risk of fraud; the expenses incurred in mitigating risks which included the cost of credit freezes, insurance, monitoring, and other

[130] *Id.* at 390 (alteration in original).
[131] *Id.* at 386.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] *Id.* at 386, 388. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).
[137] *Galaria*, 663 F. App'x at 388.
[138] *Id.* at 386.
[139] *Id.* ("Identity thieves may also use a victim's identity when arrested, resulting in warrants issued in the victim's name. . . . Plaintiffs allege that victims of identity theft and fraud will 'typically spend hundreds of hours in personal time and hundreds of dollars in personal funds,' incurring an average of $354 in out-of-pocket expenses and $1.513 it total economic loss.").

continued . . .

mitigation products; and the time spent on mitigation efforts.[140]

The Sixth Circuit used the "substantial risk" of harm standard in *Galaria*.[141] Accordingly, the Sixth Circuit concluded that the plaintiffs' allegations of an increased risk of future harm from identity theft or fraud, coupled with reasonably incurred mitigation costs, was sufficient to establish an Article III injury at the pleading stage.[142] The Sixth Circuit noted that Nationwide seemed to recognize the severity of the risks because of its offer to pay for a year of credit-monitoring and identity-theft protection.[143] The court noted that where a data breach targets personal information, "a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes."[144] It would be unreasonable for the plaintiffs to wait until after a thief misused their data to take steps to ensure their security.[145] Therefore, although it was not "literally certain" that the plaintiffs personal information would be misused, there was a substantial risk of harm that was sufficient for the plaintiffs to incur reasonable costs in mitigating an imminent harm.[146] The court determined that these reasonable costs were a concrete injury.[147] Therefore, the plaintiffs satisfied the injury-in-fact requirement of Article III standing.[148]

Additionally, the Sixth Circuit concluded that the injuries the plaintiffs alleged met both the second and third element of Article III standing.[149] As the court noted, "[a]lthough hackers are the direct cause of plaintiffs' injuries, the hackers were able to access plaintiffs' data only because Nationwide allegedly failed to secure the sensitive personal information entrusted to its custody."[150] The court determined that, but for Nationwide's poor security, the hackers would not have

[140] *Id.* at 387.

[141] *Id.* at 388. Courts have "found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," even where it is not 'literally certain the harms they identify will come about.'" *Id.* (quoting *Clapper*, 586 U.S. at 414 n.5).

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.* at 388, 389.

[147] *Id.*

[148] *Id.*

[149] *Id.* at 387–92 (explaining that the second and third elements of standing are an injury-in-fact "fairly traceable to the challenged conduct of a defendant" and "likely to be redressed by a favorable judicial decision") Plaintiffs met the second element by alleging that Nationwide failed to implement safeguards to ensure the security and confidentiality of the Plaintiffs' data. *Id.* at 390. The third element was met because the compensatory damages the Plaintiffs sought would provide redress. *Id.* at 390–91.

[150] *Id.* at 390.

continued . . .

been able to steal and misuse the plaintiffs' personal information.[151] As a result, the alleged injuries were fairly traceable to the actions of Nationwide.[152] Lastly, the court concluded that the plaintiffs successfully showed that a favorable verdict granting them compensatory damages could redress their injuries[153]

2. Lewert v. P.F. Chang's China Bistro, Inc.

In *Lewert v. P.F. Chang's China Bistro, Inc.*, a case which took place following *Clapper* and prior to *Spokeo*, the Seventh Circuit found that the plaintiffs alleged enough injury to support Article III Standing.[154] About two months after the plaintiffs, John Lewert and Lucas Kosner, dined at P.F. Chang's, they received news that the restaurant chain's computer system had been hacked, and customers' debit and credit card information was stolen.[155] Originally P.F. Chang's switched to a manual card processing system and encouraged customers to monitor their credit card statements; however, the chain later determined that the hack affected only thirty-three of the chain's restaurants.[156]

Kosner cancelled his debit card when he noticed four fraudulent transactions were made a little over a month after using his card at P.F. Chang's.[157] Subsequently, he purchased a credit monitoring service for $106.89 to protect himself against identity theft and any criminals who might open up new debit or credit cards in his name.[158] Unlike Kosner, Lewert never experienced any fraudulent charges on his card, nor did he have to cancel his card.[159] Instead, Lewert alleged that he was injured because of the time and effort he spent monitoring his card statements and credit report to ensure that no fraudulent activity took place.[160] The Seventh Circuit concluded that the plaintiffs sufficiently alleged enough injury to meet the three elements of Article III standing.[161]

The Seventh Circuit compared the facts of *Lewert* to an earlier data

[151] *Id.*
[152] *Id.*
[153] *Id.* at 391 (holding that the Plaintiff sought compensatory damages for injuries sustained and a favorable verdict would adequately redress the dispute).
[154] Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 970 (7th Cir. 2016).
[155] *Id.* at 965.
[156] *Id.*
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.* at 966.

continued . . .

breach case, *Remijas v. Neiman Marcus Group, LLC*, which also took place after *Clapper* and before *Spokeo*.[162] Similar to P.F. Chang's, Neiman Marcus experienced a data breach where many customers' private payment card data was stolen.[163] In *Remijas*, the Seventh Circuit found the plaintiffs' injuries were concrete and particularized enough to establish Article III standing.[164] The Seventh Circuit "identified two future injuries that were sufficiently imminent: the increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft."[165] The Seventh Circuit found that these two instances were not mere "allegations of possible future injury," but were instead the type of "certainly impending" future harm that the Supreme Court requires to establish standing.[166] The *Remijas* court asserted that plaintiffs "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur."[167] As a result, the court in *Lewert* held that the time and money Lewert and Kosner spent in an effort to resolve fraudulent charges were "cognizable injuries for Article III standing."[168] Thus, the court determined that Lewert and Kosner met the first element of injury-in-fact,[169] and the court quickly analyzed the last two elements of Article III standing.[170] Ultimately, the *Lewert* court reasoned that the plaintiffs pled enough facts to plausibly allege that their injuries were fairly traceable to P.F. Chang's failure to protect their payment card information.[171] Lastly, the court concluded that a favorable judgment could redress most of the plaintiffs' injuries, particularly the easily quantifiable financial injuries.[172]

---

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.* (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015)).

[166] *Remijas*, 794 F.3d at 692 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013)).

[167] *Id.* at 693 (quoting *Clapper*, 568 U.S. at 410).

[168] *Lewert*, 819 F.3d at 967.

[169] *Id.* (explaining that due to a data breach in June of 2014, a court could reasonably find that a risk of fraudulent charges would affect credit cards).

[170] *Id.* at 966.

[171] *Id.* at 969 (noting that the plaintiffs at least partially satisfied the criteria for Article III standing because "at least some of the injuries Lewert and Kosner allege[d] . . . qualify as immediate and concrete injuries sufficient to support Article III standing").

[172] *Id.* (noting that the plaintiffs also satisfied the criteria of redressability for Article III standing because they had "some easily quantifiable financial injuries" including purchasing credit monitoring services).

continued . . .

3. Resnick v. AvMed, Inc.

Six months prior to the Supreme Court's decision in *Clapper*, the Eleventh Circuit analyzed a case which was very similar to *CareFirst.* Similar to the plaintiffs in *CareFirst*, the plaintiffs in *Resnick v. AvMed, Inc.* sued AvMed, a healthcare service provider, after two laptops containing customers' sensitive information were stolen from AvMed's offices.[173] This sensitive information included protected health information, Social Security numbers, names, addresses, and phone numbers.[174] The plaintiffs alleged that AvMed failed to encrypt or secure these laptops, so the sensitive information was readily accessible when they were stolen.[175] "The unencrypted laptops contained the sensitive information of approximately 1.2 million current and former AvMed members."[176]

Unfortunately for AvMed customers, these stolen laptops were sold to an individual with a history of dealing in stolen property.[177] Plaintiffs, Juana Curry and William Moore, both experienced identity theft shortly after the laptops were stolen.[178] The thief used Curry's information to open accounts at Bank of America, activate credit cards in Curry's name, and use those credit cards to make unauthorized purchases.[179] Similarly, an identity thief used Moore's sensitive information to open an account with E*Trade Financial.[180]

The Eleventh Circuit determined that the plaintiffs met the first element of injury-in-fact because "[they alleged] that they [had] become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury-in-fact under the law."[181] This standard, that a plaintiff must actually become a victim of identity theft and suffer monetary damages, mirrors the *Clapper* Court's holding, which implied that a hacker has to steal a consumer's identity and actually participate in fraudulent activity in order for the consumer to meet the Article III injury-in-fact requirement.[182]

Next, the *Resnick* court determined that the plaintiffs' injury was

[173] Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012).
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] *Id.*
[180] *Id.*
[181] *Id.* at 1323 (alteration in original).
[182] *See generally* Martecchini, *supra* note 69, at 1479–83 (discussing standing based on risk of future harm after *Clapper*).

continued . . .

fairly traceable to AvMed's negligence.[183] The court stated: "Even a showing that a plaintiff's injury is indirectly caused by a defendant's actions satisfies the fairly traceable requirement."[184] Finally, the Eleventh Circuit determined that a favorable judicial decision awarding compensatory damages could redress the plaintiffs' alleged monetary injury.[185]

C. The Second and Fourth Circuits Find That an Increased Risk of Future Harm is Insufficient to Establish Article III Standing

1. Whalen v. Michaels Stores, Inc.

As compared to the D.C., Sixth, Seventh and Eleventh Circuit's view, the Second and Fourth Circuits have stricter views, holding that allegations of nothing more than an increased risk of future injury does not adequately support Article III standing.[186] Following *Spokeo*, the Second Circuit heard *Whalen v. Michaels Stores, Inc.*, where it found that the plaintiff-appellant, Mary Jane Whalen, failed to allege a cognizable injury after her credit card information was exposed following a data breach of Michaels' computer system.[187] The Second Circuit upheld the district court's holding that Whalen failed to allege an injury, and therefore, Whalen did not meet the injury-in-fact element of Article III standing.[188]

Whalen asserted three theories of injury in her case: "(1) her credit card information was stolen and used twice in attempted fraudulent purchases; (2) she face[d] a risk of future identity fraud; and (3) she has lost time and money resolving the attempted fraudulent charges and monitoring her credit."[189] However, Whalen's first theory of injury failed because she never suffered any monetary harm from the attempted fraudulent charges because she was neither asked to pay, nor did she pay, any fraudulent charge.[190] The Second Circuit found that

[183] *Resnick*, 693 F.3d at 1323.
[184] *Id.*
[185] *Id.*
[186] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (holding that the plaintiff lacked standing because she neither incurred any actual charges on her credit card nor spent time or money monitoring her credit); Beck v. McDonald, 848 F.3d 262, 266–67 (4th Cir. 2017) (holding that harm from the increased risk of future identity theft and costs of the measures to protect from harm failed to establish a non-speculative, imminent injury-in-fact to meet standing requirements).
[187] *Whalen*, 689 F. App'x at 89.
[188] *Id.* at 90.
[189] *Id.* (alteration in original).
[190] *Id.*

continued . . .

Whalen's second theory of injury failed because she immediately cancelled her credit card after the breach, and no other sensitive personal information was stolen in the breach.[191] The court determined that therefore, Whalen could not possibly face a risk of future identity fraud purely from hackers stealing her cancelled credit card information.[192] Lastly, Whalen's third theory of injury failed because she did not allege with any specificity the amount of money and time she spent monitoring her credit.[193] The Second Circuit held that the mere allegation that she spent time and money monitoring her credit, without any specifics, was not substantial enough to establish an injury-in-fact.[194]

Although, the Second Circuit appeared to conclude that an increased risk of future harm is insufficient to support Article III standing, it is possible the court would have found standing if a couple of facts were changed. For example, if Whalen had been more specific about the time and money she lost in monitoring her credit, the Second Circuit may have ruled differently.[195] The opinion also took the time to distinguish Whalen's circumstances from the plaintiffs in *Galaria*.[196] The Second Circuit noted that unlike the plaintiffs in *Galaria*, none of Whalen's personal information, such as her birthdate or Social Security number, were alleged to have been stolen.[197] If Whalen's sensitive personal information had been compromised in the breach, it seems more likely that the Second Circuit would have found that Whalen faced a risk of future identity fraud to establish the first element of injury-in-fact.

---

[191] *Id.*

[192] *See id.*

[193] *Id.* at 91.

[194] *Id.*

[195] *See id.*; *cf.* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) ("Similarly, [plaintiffs] have alleged sufficient facts to support standing based on their present injuries. Kosner asserts that he already has experienced fraudulent charges. Even if those fraudulent charges did not result in injury to his wallet (he stated that his bank stopped the charges before they went through), he has spent time and effort resolving them. He also took measures to mitigate his risk by purchasing credit monitoring for $106.89. Lewert alleged that he has spent time and effort monitoring both his card statements and his other financial information as a guard against fraudulent charges and identity theft." (alteration in original)).

[196] *Compare Whalen*, 689 F. App'x at 90 (finding no standing where the stolen credit card was immediately cancelled and no other personal identifying information was alleged as stolen), *with* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016) (finding standing where the breached database contained personal information such as names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers).

[197] *Whalen*, 689 F. App'x at 90.

continued . . .

2. Beck v. McDonald

Following *Spokeo*, the Fourth Circuit heard *Beck v. McDonald*, where it found that the "[p]laintiffs failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing."[198] The plaintiffs brought suit against the William Jennings Bryan Dorn Veterans Affairs Medical Center (the "Center") in Columbia, South Carolina, after two data breaches at the Center compromised the plaintiffs' personal information.[199] The first data breach occurred after a laptop connected to a pulmonary function testing device was misplaced or stolen from the hospital.[200] The laptop contained "unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of Social Security numbers, and physical descriptors of patients."[201] The plaintiffs alleged "that the 'threat of identity theft' required them to frequently monitor their 'credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial accounts.'"[202]

The second breach occurred after four boxes of pathology reports were misplaced or stolen at the Center.[203] These reports contained "identifying information of over 2,000 patients, including names, Social Security numbers, and medical diagnoses."[204] Similar to the first breach, the Fourth Circuit found that the plaintiffs "'ha[d] not alleged that there ha[d] been any actual or attempted misuse of her personal information,' thus rendering her allegation that her information 'will eventually be misused as a result of the disappearance of the boxes . . . speculative.'"[205] The *Beck* court determined that the threat of future harm was based on an "attenuated chain of possibilities[,]" and therefore, it was not an imminent injury under the first element of Article III standing.[206]

Further, the Fourth Circuit distinguished the data breaches at the Center from the data breaches experienced in *Galaria* and *Remijas*.[207] In *Galaria* and *Remijas*, the data thief intentionally targeted the personal

[198] Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017).
[199] *Id.* at 266.
[200] *Id.*
[201] *Id.* at 267.
[202] *Id.* (alteration in original).
[203] *Id.* at 268.
[204] *Id.*
[205] *Id.* at 269 (alteration in original).
[206] *Id.*
[207] *Id.* at 273.

continued . . .

information compromised in the data breach.[208] In other words, the data thief hacked these two companies with the sole purpose of obtaining consumers' sensitive personal information.[209] In contrast, the plaintiffs in both of the *Beck* data breaches, provided no evidence that information contained on the misplaced or stolen laptop and boxes of pathology reports were accessed or misused by someone with an ill-motive, or that the plaintiffs suffered identity theft.[210] The court stated: "'[A]s the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative."[211]

The court determined that although the laptop and boxes containing pathology records were stolen, the plaintiffs must provide more evidence of an injury in order to obtain Article III standing.[212] In conclusion, the Fourth Circuit is not nearly as plaintiff friendly as the D.C., Sixth, Seventh, Eleventh Circuits, or even the Second Circuit, when it comes to granting Article III standing based on the increased risk of future harm.

D. Courts Should Find That Equifax Victims Meet All Three Elements Required to Establish Article III Standing

Although the circuit courts remain split in regards to whether the increased risk of identity theft is enough to constitute Article III standing, it is likely that if the Equifax victims bring a claim in the D.C., Sixth, Seventh, Eleventh, or even the Second Circuit, the victims will be successful in pleading an injury-in-fact that will satisfy Article III standing. First, the Equifax victims will have to prove that the information stolen in the breach creates a concrete and particularized injury that is actual or imminent, and not conjectural or hypothetical.[213] In order to meet this requirement, victims will need to plead facts that describe in detail their incurred monetary losses, as well as the amount of time spent monitoring their financial well-being.

The circuits have agreed that where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for fraudulent purposes.[214] Thus, it would be

[208] *Id.* at 274.
[209] *Id.*
[210] *Id.*
[211] *Id.* at 275 (quoting Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564, 570 (D. Md. 2016)).
[212] *See id.* at 266–67.
[213] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).
[214] Attias v. CareFirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017); *Galaria*, 663 F. App'x at 388; Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); *see* Resnick v. AvMed, Inc., 693 F.3d 1317, 1330 (11th Cir. 2012)

continued . . .

unreasonable for affected consumers to wait until after a thief misused their data to take steps to ensure their security.[215] So, although it is not "literally certain" that the consumers personal information will be misused, "there is a sufficiently substantial risk of harm" for plaintiffs to incur reasonable costs in mitigating an imminent harm.[216] These reasonable costs are considered to be a concrete injury.[217] Like the victims in *CareFirst*, *Galaria*, and *Resnick*, whose personal information was stolen, the Equifax victims' hypersensitive personal information like Social Security numbers were compromised.

In *Whalen*, the Second Circuit seemed to suggest that if a victim's Social Security number is stolen, the victim will have a greater chance of establishing a substantial risk of future harm.[218] This is because, unlike a credit card number, a Social Security number cannot be cancelled or changed. Therefore, the identity theft victim has no choice but to spend the rest of their life closely monitoring their financials. As a result, it is likely that even if Equifax victims found themselves in the Second Circuit, they have a chance of success.

Although Equifax offered a free year of credit monitoring and identity theft protection services to consumers, as well as waived the freeze fee until November 2017, Equifax victims will eventually be forced to incur costs for freezing and unfreezing their credit. They will also have to pay for the credit monitoring and identity theft protection services after their free year has expired. The threat of identity theft does not just disappear after a year.[219] Hackers can use sensitive personal information, such as a Social Security number, indefinitely.[220] It is possible that Equifax victims may be fighting off identity theft and fraud for the rest of their lives. Thus, many victims will likely be able to plead that they have incurred reasonable costs in mitigating the future

(holding that a "sufficient nexus" between a data breach and fraudulent use of personal information constitutes a requisite injury); *see also* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (reasoning that there was insufficient injury, partly because the plaintiff had quickly canceled her credit card following a breach).

[215] *Galaria*, 663 F. App'x at 388.

[216] *Id.*

[217] *Id*. at 389.

[218] *See generally Whalen*, 689 F. App'x at 89 (stating that plaintiff failed to allege a threat of future fraud because her Social Security number was not stolen).

[219] Maurie Backman, *Will the Equifax Data Breach Impact Your Social Security Benefits?*, USA TODAY (Sept. 15, 2017), https://www.usatoday.com/story/money/personalfinance/2017/09/15/will-the-equifax-data-breach-impact-your-social-security-benefits/105616332/.

[220] Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N BLOG (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do?page=4.

continued . . .

harm of identity theft and fraud. Therefore, Equifax victims should be able to satisfy the first element of injury-in-fact.

Similar to the plaintiffs' information in *CareFirst*, *Galaria*, *Lewert*, and *Resnick*, the Equifax victims' information was intentionally stolen by hackers looking to breach the company's computer system. This element of "intent" is what the Fourth Circuit used to distinguish the facts described in *Beck* because, in that instance, there was no evidence that the laptops or boxes of records were intentionally stolen with the purpose of stealing patients' personal information.[221] Because of this, the Fourth Circuit concluded that the injuries alleged by the plaintiffs were too speculative.[222] However, the Equifax victims can distinguish their circumstances from those plaintiffs in *Beck* because the breach of Equifax's computer system aligns more closely with the breaches described in *CareFirst*, *Galaria*, *Lewert*, *Resnick*, and *Whalen*, where the hackers intentionally breached the computer systems with the goal of acquiring customers' personal information.[223]

The Equifax victims should have no problem establishing that their injury is fairly traceable to Equifax, the second element of Article III standing. Equifax already conceded that the data breach was caused by its failure to patch a technological flaw in their software, even after it was put on notice of the flaw.[224] Equifax will likely argue that they cannot be held responsible because the hacker would be the most immediate cause of the victims' injuries. However, the D.C. Circuit in *CareFirst* found that although the company's failure to secure its customers' sensitive data was one step removed in the causal chain, the injury was still "fairly traceable" to CareFirst.[225] Thus, it is likely that courts could conclude that although the hackers are the immediate cause of the Equifax victims' injuries, the Equifax victims' increased risk of identity theft is fairly traceable to Equifax's failure to adequately secure victims' private information.

Equifax victims should have no problem satisfying the third element of Article III standing. As long as the victims specifically identify the reasonable costs they have incurred in responding and attempting to mitigate the data breach, the court should find that they can be made

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

[222] *Id.* at 277–78.

[223] *See generally* text accompanying *supra* notes 220–223 (explaining that the Equifax victims suffered from a breach of hypersensitive personal information similar to the victims in *CareFirst*, *Galaria*, and *Resnick*); *see generally* text accompanying *supra* note 228 (explaining that the Equifax victims suffered from an intentional breach by hackers similar to the breaches in *CareFirst*, *Lewert*, and *Resnick*).

[224] Sweet & Liedtke, *supra* note 8.

[225] Attias v. CareFirst, 865 F.3d 620, 629 (D.C. 2017).

continued . . .

whole again by monetary damages; the victims' injuries would be redressed by a favorable judicial decision.

The Equifax victims are different than many of the plaintiffs in the aforementioned cases because they did not explicitly consent to Equifax collecting their personal information. In *CareFirst*, *Galaria*, *Resnick*, *Whalen*, *Lewert*, and *Beck*, the victims were direct customers of the companies from which their personal information was stolen.[226] The victims of those breaches voluntarily offered up their personal information to that company when they purchased the company's goods or services.[227] However, this does not stand true for the entirety of the 147.9 million Equifax victims.[228] Many of the victims were not direct customers of Equifax and were unaware of the information that Equifax had collected.[229] This distinguishes the Equifax victims from any of the previously mentioned data breach cases' victims and may be helpful in pleading their case.

Ultimately, it appears that Equifax victims may have a very good chance of establishing standing. The facts of their case are extremely similar to, and even stronger than, any of the aforementioned cases. However, the lack of uniformity among circuits makes it difficult to predict the certainty of victims' success. Victims that are able to show that their information was actually misused, and that fraudulent activity took place will likely be the most successful. Nonetheless, victims who have not yet experienced identity theft or fraud may still have a chance in holding Equifax accountable for its negligence in failing to safeguard their personal information.

IV. CONCLUSION

Due to the fact that the circuit split remains unresolved and data breach litigation is steadily increasing, the Supreme Court needs to address the issue and determine whether an increased risk of future injury, such as identity theft and fraud, satisfies the injury-in-fact requirement of Article III standing. The uncertainty caused by the circuit split makes it unclear as to whether victims of data breaches will be successful in their suits. Additionally, the circuit split raises the cost of litigation for all and increases the potential risk of liability for

[226] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017); text accompanying *supra* notes 103–06, 135, 160–61, 179.

[227] *See generally* text accompanying *supra* note 231 (implying that when a customer engages in a business transaction the customer gives consent to collect their information to the business they are engaged with).

[228] Schneier, *supra* note 15; Clements, *supra* note 12.

[229] Schneier, *supra* note 15.

continued . . .

companies facing class action suits based on allegations of increased risk of identity theft after a data breach.[230]

If the Supreme Court were to finally hear a case involving a corporate data breach and the increased risk of identity theft, there are many things the Court should consider. Failing to determine that an increased risk of identity theft or fraud is an injury-in-fact suitable to establish standing, is a dangerous precedent to set for consumers, and provides large corporations, like Equifax, with little incentive to vigorously protect the sensitive information of consumers.

In addition to the Supreme Court taking action to resolve the circuit split, legislators should fight for the American people and create laws that protect American's sensitive personal information from the indifference and negligence of corporations. Moreover, legislators need to make it possible for consumers to have more control over their personal information. The Equifax breach illuminated the fact that many corporations possess the sensitive information of Americans sometimes without their consent and do very little to protect the information from malicious hackers or individuals with ill-motives.[231] This lack of required consent makes it impossible for Americans to protect themselves against identity theft and fraud.

In the wake of Equifax's massive plunder, many politicians have come forth with solutions.[232] For example, Senator Elizabeth Warren, proposed a bill that would give all Americans access to free credit freezing and unfreezing for life.[233] Although this is a step in the right direction, it does nothing to hold corporations accountable for failing to take reasonable steps in safeguarding consumers' personal information. Additionally, because of the digital age we live in, it is likely time the government creates an agency with the sole task of regulating, auditing, and fining corporations who fail to meet the agency's imposed safety standards. If the government really wants to see a change in

[230] McNicholas & Nye, *supra* note 95.

[231] *See generally* Paresh Dave, *Facebook Scandal Could Push Other Tech Companies to Tighten Data Sharing*, REUTERS (Mar. 22, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica-apps/facebook-scandal-could-push-other-tech-companies-to-tighten-data-sharing-idUSKBN1GY0F5 (discussing how Facebook allowed Cambridge Analytica, a British election consulting firm, to access data on 50 million Facebook users and use the data to help the election campaign of President Donald Trump).

[232] *See, e.g.*, Freedom from Equifax Exploitation Act, S. 1816, 115th Cong. (2017); PROTECT Act of 2017, H.R. 4028, 115th Cong. (2017); Brian Eason, *Colorado Lawmakers Look to Bolster Consumer Protections After Equifax Breach*, DENVER POST (Jan. 22, 2018, 4:30 PM), https://www.denverpost.com/2018/01/22/colorado-lawmakers-bolster-consumer-protections-after-equifax-breach/.

[233] Adam Levin, *Post Equifax: Will Free Credit Freezes Help?*, USA TODAY (Sept. 27, 2017, 10:30 AM), https://www.usatoday.com/story/money/personal finance/2017/09/27/post-equifax-free-credit-freezes-help/701883001/.

corporations' responses to cybersecurity, it should create laws and regulations that impose massive fines on corporations who fail to safeguard consumer information.