Journal of Law and Policy

Volume 28 | Issue 1 Article 3

12-1-2019

Increasing Lapses in Data Security: The Need for a Common Answer to What Constitutes Standing in a Data Breach Context

Aaron Benjamin Edelman

INCREASING LAPSES IN DATA SECURITY: THE NEED FOR A COMMON ANSWER TO WHAT CONSTITUTES STANDING IN A DATA BREACH CONTEXT

*Aaron Benjamin Edelman**

A liberal application of standing doctrine in the data breach context will create stronger preventative protections to personal information and provide remedies should those protections fail.

INTRODUCTION

In 2017, individuals and entities in the United States fell victim to the greatest number of data breaches in statistical history.[1] Data breaches are difficult to both define and enumerate. In the United States, each state has enacted legislation which requires "private or governmental entities to notify individuals about security breaches of personally identifiable information."[2] Each of these data breach notification laws defines, to varying degrees of inclusivity, what a data breach is under that state's code, enumerates what personal information falls within its scope such that the putting at risk of that

---

* J.D. Candidate, Brooklyn Law School, 2020; B.B.A, University of Wisconsin-Madison, 2017. Thank you to my parents and siblings for providing an overwhelming amount of support and encouragement in everything I do. Additionally, thank you to each and every member of the *Journal of Law & Policy* for the insight and counsel that made this Note possible.

[1] J. Clement, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018 (in millions)*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last updated Aug. 5, 2019).

[2] *Security Breach Notification Laws*, NSCL (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

information qualifies as a data breach,[3] determines which institutions are subject to compliance with the law,[4] sets out requirements for notice,[5] and provides exemptions.[6] Public disclosure of data breaches, while expected and often required of compromised institutions by state data breach notification laws, is not done every time a breach occurs, so with that understanding, only publicly available information can form the basis of these statistics. In 2018, "[h]acking was the most common form of data breach[;]"[7] hacking is defined by Merriam-Webster as "an act or instance of gaining or attempting to gain illegal access to a computer

---

[3] ME. REV. STAT. ANN. tit. 10, § 210-1347 (2005).

> "Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: A. [s]ocial security number; B. [d]river's license number or state identification card number; C. [a]ccount number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; D. [a]ccount passwords or personal identification numbers or other access codes; or E. [a]ny of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

Id. (internal citations omitted).

[4] UTAH CODE ANN. § 13-44-202 (West 2019). "A person who owns or licenses computerized data that includes personal information concerning a Utah resident" is subject to the law. *Id.* § 13-44-202 (1)(a).

[5] S.C. CODE ANN. § 39-1-90 (2019). Notice is required to residents or persons doing business in the state if "illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm" to the person or business. An exemption to notice is when disclosure would "impede[] a criminal investigation." *Id.* § 39-1-90 (B)–(D)(1).

[6] *Security Breach Notification Laws*, *supra* note 2.

[7] IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT 2 (2018), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf. Other forms of data breaches include human error, and theft, or loss of a device. *Id.* at 10.

or computer system."[8] While each state's code defines what a breach is in various ways, generally speaking, all statutes cover some form of unauthorized acquisition of personal information.[9] Hacking by Merriam-Webster's definition falls into the direct ambit of what data breach notification laws target.[10] Hacking's large role in data breaches is concerning because hackers generally obtain stolen information to use in fraudulent activity.[11] In 2016, hackers breached the Internal Revenue Service's ("IRS") data retrieval tool, which parents used to transfer financial information for their college-bound children applying for federal aid; the hackers stole thirty million dollars from the IRS after posing as college students to obtain fraudulent tax refunds.[12] Furthermore, there is no indication that the number of data breaches which come about as a result of hacking is likely to decline in the near future, as evidenced by the over 1,244 publicly reported data breaches in 2018—a dramatic increase from the mere 157 known data breaches in 2005.[13] The growing threat of data breaches is further evidenced by the fact that the number of reported breaches in 2019 is up 56.4%, and the number of exposed records is up 28.9% from the first quarter of 2018.[14]

---

[8] *Definition of Hack*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/hack (last visited Sept. 18, 2019).

[9] *See generally* Jennifer J. Hennessy et al., *State Data Breach Notification Laws*, FOLEY & LARDNER LLP (July 1, 2019), https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws (citing to an internal State Date Breach Notification Laws Chart, which includes a definition of personal information for each state).

[10] *See, e.g.*, FLA. STAT. § 501.171 (2019) (defining a security breach as "the unauthorized access of data in electronic form containing personal information"); *Definition of Hack*, *supra* note 8.

[11] *See What Do Hackers Do With Your Stolen Identity?*, TREND MICRO (June 21, 2017), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity.

[12] Alfred Ng, *Hackers Use College Student Loans Tool to Steal $30 Million*, CNET (Apr. 7, 2017, 10:15 AM), https://www.cnet.com/news/hackers-used-college-student-loans-tool-to-steal-30-million/.

[13] J. Clement, *supra* note 1.

[14] *Data Breach Trends in 2019*, SECURITY MAG. (May 8, 2019), https://www.securitymagazine.com/articles/90207-data-breach-trends-in-2019.

The value of personal information in the modern digital world makes it a highly coveted asset for hackers and other nefarious parties. Hackers often target personally identifiable information, which (depending on state definitions) frequently includes sensitive financial and healthcare information.[15] This stolen information can be used, for instance, to take out loans, make fraudulent credit card transactions, and fill prescriptions illegally.[16] Once stolen, hackers typically turn to underground markets such as those on the dark web to sell the stolen data.[17] The data is then either sold individually, in bulk, or in a bundle of various types of stolen information.[18] Affected by this growing underground market for stolen information, United States citizens continue to fall victim to hundreds of thousands of reported cases of identity theft.[19]

Victims of data breaches frequently turn to the law as a remedy.[20] In 2018, "5.7% of data breaches publicly reported led to

---

[15] *What Do Hackers Do With Your Stolen Identity?*, *supra* note 11.

[16] *Id.*

[17] *Id.*; *see* Ellen Sirull, *What is the Dark Web?*, EXPERION (Apr. 8, 2018), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ ("The dark web isn't an actual place, but rather a hidden network of websites."); *see also* Brian Stack, *Here's How Much Your Personal Information is Selling For On The Dark Web*, EXPERION (Apr. 9, 2018), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ ("After a data breach or hacking incident, personal information is often bought and sold on the dark web by identity thieves looking to make money off your good name—and any numbers or information associated with you.").

[18] Stack, *supra* note 17.

[19] *See Facts + Statistics: Identity Theft and Cybercrimes*, INS. INFO. INST. (2019), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime ("The Consumer Sentinel Network, maintained by the Federal Trade Commission (FTC), tracks consumer fraud and identity theft complaints that have been filed with federal, state and local law enforcement agencies and private organizations."). In 2018, there were 444,602 identity theft complaints, whereas in 2016 there were 398,952 identity complaints. *Id.*

[20] *See, e.g.*, *In re* SuperValu Inc., 870 F.3d 763, 773 (8th Cir. 2017); Attias v. CareFirst Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 277–78 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015) (demonstrating various instances wherein victims of data breaches filed lawsuits against entities responsible for protecting their personal information).

class action litigation[,] . . . indicating a steady increase in class action litigation relative to the number of breaches."[21] This increase in litigation will likely continue as hackers target personal information, recognizing its market value.[22] Many potential plaintiffs who suffered as victims of data breaches, however, find themselves in limbo regarding the issue of standing before a court because of a significant split amongst the federal circuit courts.[23] Thus, while victims of data breaches oftentimes have their personal information fall into the hands of nefarious characters who intend to use the information to the victims' detriment, that may not be enough to provide victims a right to sue in federal court because of disparate interpretations of standing that create impediments to data breach litigation.[24]

Standing is a determination of whether or not someone has grounds to bring suit based on the contextual reading of Article III of the United States Constitution.[25] Article III, which governs federal courts, places a limit on the judiciary and dictates that federal courts can only hear "cases" and "controversies" that are

---

[21] DAVID ZETOONY ET AL., 2019 DATA BREACH LITIGATION REPORT 2 (2019), https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf [hereinafter ZETOONY ET AL., 2019 DATA BREACH LITIGATION REPORT].

[22] *See* DAVID ZETOONY ET AL., 2017 DATA BREACH LITIGATION REPORT 8 (2017), https://www.bclplaw.com/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf [hereinafter ZETOONY ET AL., 2017 DATA BREACH LITIGATION REPORT].

[23] *See, e.g.*, *In re SuperValu Inc.*, 870 F.3d at 773; *Attias*, 865 F.3d at 629; *Whalen*, 689 F. App'x 89; *Beck*, 848 F.3d at 277–78; *Galaria*, 663 F. App'x at 387–89 (showing how various circuits have reached differing conclusions on the standard for establishing standing for victims of data breaches).

[24] *See, e.g.*, *In re SuperValu Inc.*, 870 F.3d at 773; *Attias*, 865 F.3d at 629; *Whalen*, 689 F. App'x 89; *Beck*, 848 F.3d at 277–78; *Galaria*, 663 F. App'x at 387–89 (6th Cir. 2016); *Remijas*, 794 F.3d at 690 (exhibiting how the absence of a uniform rule evaluating standing in a data breach context, with respect to the harm suffered by plaintiffs, will continue to create conflicting results and uncertainty amongst plaintiffs as to whether their harms are redressable).

[25] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (citing Allen v. Wright, 468 U.S. 737, 751 (1984)) ("[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III."); *see* U.S. CONST. art. III, § 2.

"traditionally amenable to, and resolved by, the judicial process."[26] The standing requirements have been broken down into: (1) an injury in fact, (2) redressability, and (3) a causal connection between the injury suffered and the matter brought into court.[27] An injury in fact is a harm that is "concrete and particularized" and "actual or imminent."[28] Therefore, an injury cannot be "conjectural or hypothetical."[29] However, a harm suffered is not limited to physical harms; it includes violations of personal rights.[30] The injury in fact must also be redressable in that courts must have the ability to offer a remedy for the injury sustained.[31] Finally, the injury suffered must have a causal connection to the matter brought into court—the injury must be "fairly traceable" to the challenged action of the defendant.[32] As these factors leave room for interpretation on a case-by-case basis, a uniform determination of standing is increasingly necessary as data breach litigation has become more commonplace, accompanied by an increased number of victims facing an impediment to recourse in the legal system.[33]

In a data breach context, plaintiffs typically file a data breach suit when they entrust a person or entity with personally identifiable information (such as social security numbers, credit card information, home address, or different combinations of personally identifiable information as enumerated on a state-by-state basis) and a third party steals that information.[34] Plaintiffs often sue the trusted entity that failed to protect their personal information based on a potential future harm that may occur because of lackluster

---

[26] U.S. CONST. art. III, § 2, cl. 1; Vt. Agency of Nat. Res. v. United States *ex rel.* Stevens, 529 U.S. 765, 774 (2000) (internal quotation marks omitted).

[27] *Lujan*, 504 U.S. at 560–61.

[28] *Id.* at 560.

[29] *Id.*

[30] *Id.* at 564 n.2.

[31] *Id.* at 561.

[32] *Id.* at 560.

[33] *See* ZETOONY ET AL., 2017 DATA BREACH LITIGATION REPORT, *supra* note 22, at 2 ("[P]laintiffs continue to face [difficulty] establishing that they were injured by a breach and, therefore, have standing as a matter of law to bring suit.").

[34] *See Data Breach Lawsuit*, CLASS ACTION.COM, https://www.classaction.com/data-breach/lawsuit/ (last updated Nov. 30, 2018).

security.[35] If third party hackers use the stolen information against a plaintiff, there is a stronger case for standing because a concrete and easily elucidated harm has been suffered.[36] However, in cases where the alleged harm is a future harm—where plaintiffs plead a "certainly impending" injury or a substantial risk of injury—circuits are split as to what constitutes an "injury in fact" and when to find a causal connection between the theft and future harm.[37] The split makes it unclear if plaintiffs have suffered an "injury in fact" at the time when their personal information is stolen or if victims of the breach must wait until that stolen information is used to their detriment.[38]

As data breaches and data breach litigation become more common, it is increasingly important that courts establish a uniform application of the standing doctrine.[39] In the first three months of 2019, approximately two billion data records are known to have been compromised worldwide—a drastic increase in stolen records from 2018 when five billion data records were compromised in the entire calendar year.[40] The number of lawsuits related to sensitive information will likely continue to grow as companies increasingly collect data and personal information to better understand consumers, and as hackers become more sophisticated.[41] Currently,

---

[35] *Id.*

[36] *See In re* SuperValu, Inc., No. 14-MD-2586 (ADM/TNL), 2016 WL 81792, at *6 (D. Minn. Jan. 7, 2016).

[37] *See* Dominic Spinelli, *Data Breach Standing: Recent Decisions Show Growing Circuit Court Split*, PEABODY ARNOLD (Aug. 31, 2017), https://www.peabodyarnold.com/data-breach-standing-recent-decisions-show-growing-circuit-court-split/.

[38] *Id.*

[39] *See Data Breaches Compromised 4.5 Billion Records in First Half of 2018*, GEMALTO (Oct. 9, 2018), https://www.gemalto.com/press/pages/data-breaches-compromised-4-5-billion-records-in-first-half-of-2018.aspx.

[40] *2018 Saw 6,515 Reported Breaches, Exposing 5 Billon Sensitive Records*, HELP NET SECURITY (Feb. 18, 2019), https://www.helpnetsecurity.com/2019/02/18/2018-reported-breaches/; *3 Months, 1900 Reported Breaches, 1.9 Billion Records Exposed*, HELP NET SECURITY (May 9, 2019), https://www.helpnetsecurity.com/2019/05/09/2019-publicly-reported-breaches.

[41] Bob Keaveney, *As Hackers Get More Sophisticated, Businesses Should Focus on Fundamentals*, BIZTECH (Aug. 21, 2019),

personal information is being utilized by retailers, social media companies, financial institutions, healthcare organizations, and scores of other businesses as a powerful tool to understand users and consumers.[42] To run through a series of the myriad examples, social media companies and search engines like Google and Facebook often utilize personal information so that marketers can better target consumers in the digital advertising space.[43] Data from personal cellular devices can be sold to telecommunications groups.[44] That personal data is then organized and used to determine customer traits and behavioral traits.[45] Data brokers subsequently sell large amounts of compiled data to companies, non-profits, and fundraisers.[46] Data collection has also become an invaluable part of the medical field,[47] where health insurers have made access to files for patients, prescription refills, and scheduling appointments more efficient, decreasing health insurance costs as a result.[48] Personal data further enables medical professionals to find correlations between prescription drugs and their potential effects.[49] Various entities collect personal information that people turn over, oftentimes in exchange for free access to a website or application, without the users necessarily understanding the purposes for which their

---

https://biztechmagazine.com/article/2019/08/hackers-get-more-sophisticated-businesses-should-focus-fundamentals; *see also* Louise Matsakis, *We're All Just Starting to Realize the Power of Personal Data*, WIRED (Dec. 28, 2018, 7:00 AM), https://www.wired.com/story/2018-power-of-personal-data/ (indicating how individuals use search engines or social media while unaware of how major corporations spend billions of dollars to acquire their personal data).

[42] Maryanne Gaitho, *How Applications of Big Data Drives Industries*, SIMPLI LEARN, https://www.simplilearn.com/big-data-applications-in-industries-article (last updated Aug. 26, 2019).

[43] Jeff Desjardins, *How Much is Your Personal Data Worth?*, VISUAL CAPITALIST (Dec. 12, 2016), http://www.visualcapitalist.com/much-personal-data-worth/.

[44] *Id.*

[45] *See* MARC VAN LIESHOUT, THE VALUE OF PERSONAL DATA 5 (2015), https://hal.inria.fr/hal-01431593/document.

[46] *See id.* at 3–4, 6.

[47] *Id.* at 5.

[48] *Id.* at 4–5.

[49] *Id.* at 4.

information is collected.[50] In exchange for access to a website's features or content, entities can require that cookies (site trackers that follow users from website to website) be turned on.[51] The vast collection of information has created a belief amongst Americans that they cannot control how personal information is used by the entities that collect their information.[52] In a 2017 PEW survey, only nine percent of Americans were "very confident" social media companies would protect their data, signifying the complete absence of trust in social media companies.[53]

In short, the market for personal information has become a booming industry and one over which Americans feel they have little control.[54] The Data Driven Marketing Institute[55] performed a study to determine the value of individual level consumer data ("ILCD") in the United States.[56] In 2012, the market for ILCD was worth approximately $156 billion and was responsible for 676,000 jobs.[57] But as personal information continues to increase in value, create more jobs, and slip from the control of the individuals behind that personal information, it also presents an increased value to thieves and hackers. As more personal information is collected and

---

[50] *The Value of Personal Information Nowadays*, EXPLORING YOUR MIND (Sept. 16, 2018), https://exploringyourmind.com/value-personal-information-nowadays/.

[51] *See* Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who is Using it)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/.

[52] *See* Lee Raine, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RES. CTR. (Mar. 27, 2018), https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/ ("Overall, a 2014 survey found that 91% of Americans 'agree' or 'strongly agree' that people have lost control over how personal information is collected and used by all kinds of entities.").

[53] *Id.*

[54] LIESHOUT, *supra* note 45, at 3–5; *see* Raine, *supra* note 52.

[55] *Data-Driven Marketing Institute*, DATA MARKETING & ANALYTICS, https://thedma.org/advocacy/data-driven-marketing-institute/ (last visited Sept. 18, 2019) (The Data-Driven Marketing Institute's role is to inform individuals and policymakers about how responsible data-driven marketing works, the countless ways that it benefits consumers, and the economic benefits it holds.).

[56] LIESHOUT, *supra* note 45, at 3.

[57] *Id.*

left vulnerable to third party hackers, the amount of viable litigation brought against entities entrusted with personal information will increase.[58] It follows, then, that entities possessing personally identifiable information need to prepare to take adequate preventive measures to protect themselves from litigation costs.[59] Data breach cases have the potential to create large scale putative class actions, which in turn may lead to costly settlements or large awards for plaintiffs.[60] Entities should prepare for a resolution to a current circuit split regarding when the harm suffered by data breach victims is sufficient to establish standing. A more liberal interpretation of harm that accounts for the increased risk of harm to data breach victims expands the potential class of plaintiffs who have standing to bring suit and will necessitate the just increase in information-holding entities' costs in defending or settling suits.

This Note examines conflicting holdings of various circuits on issues of standing in data breach contexts and proposes a uniform solution.[61] It posits that applying the "heightened risk of harm" standard to standing would allow victims of stolen personal information to seek recourse in a reasonable set of situations without placing an unfair burden on the breached entities to defend against an avalanche of lawsuits.[62] A "heightened risk of harm" standard

---

[58] David Balser et al., *INSIGHT: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019, 4:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch ("As we move into the second quarter of [2019], we can expect that not only will data breaches remain a common occurrence, but the scale of litigation and regulatory investigations directed towards data security will continue to expand.").

[59] *See id.*

[60] ZETOONY ET AL., 2017 DATA BREACH LITIGATION REPORT, *supra* note 22, at 5.

[61] *See, e.g.*, *In re* SuperValu, Inc., 870 F.3d 763, 773 (8th Cir. 2017); Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016) (evidencing how different circuits have been unable to articulate a uniform standard for establishing standing for victims' data breaches).

[62] *See* TRAVIS LEBLANC & JON. R. KNIGHT, A WAKE-UP CALL: DATA BREACH STANDING IS GETTING EASIER 4 (2018),

would consistently create uniformity in the courts by placing entities that are responsible for the personally identifiable information of others (as defined by each state's data breach notification statute) on notice that they need adequate security measures to guard against breaches and that they must prepare for lawsuits should those measures be lacking, even if personally identifying information has yet to be used.[63]

Part I of this Note will provide background on the standing doctrine and the repercussions of conflicting circuit court rulings on standing. Part II will examine holdings by the Fourth Circuit in *Beck v. McDonald* and the Second Circuit in *Whalen v. Michaels Stores Inc.*, both cases in which victims of stolen information were found to not have standing until and unless their personal information was used to their detriment.[64] Part III will discuss holdings that found plaintiffs who were the victims of a data breach to have standing. This Part will review the Eighth Circuit's decision in *In re SuperValu*, where it was found that a de minimis harm constitutes standing in a data breach context.[65] This Part will also analyze the decision by the Third Circuit in *In re Horizon Healthcare Services Inc. Data Breach Litigation*, where it was held that a statutory violation creates an injury in fact.[66] Additionally, this Part will examine holdings by the D.C., Sixth, and Seventh Circuits which determined that victims have standing to sue when they are at a

---

https://www.bsfllp.com/images/content/2/9/v2/2995/2018-01-17-Cyber-Security-Wake-Up-Call-Data-Breach-Standing-Is.pdf.

[63] *See* Lexi Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKLEY TECH. L.J. 1008, 1029 (2014). *See generally* Hennessy et al., *supra* note 9 (providing a comprehensive list state data breach notification laws).

[64] *See generally Whalen*, 689 F. App'x 89 (discussing what harms are sufficient to satisfy the injury in fact prong of standing analysis); *Beck*, 848 F.3d 262 (explaining how data breaches are "too speculative" to "constitute an injury-in-fact").

[65] *See generally In re SuperValu, Inc.*, 870 F.3d 763 (explaining the degree of harm necessary to satisfy the injury in fact prong of standing analysis and finding that the customer had standing).

[66] *See generally In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017) (articulating how a statutory violation can satisfy the injury in fact prong of standing analysis).

"heightened risk of harm." Finally, Part IV will consider why the Supreme Court should accept the "heightened risk of harm" standard as the universal standard in order to encourage companies to put stronger safeguards in place and provide victims of data breaches an adequate opportunity to file suit. While a statutory solution is a possibility, policy preferences amongst congressmen that either favor a pro-business or pro-consumer agenda present an obstacle to legislation.[67] Partisanship in Congress is particularly apparent in the data breach context, where several bills that would have imposed stricter requirements on businesses to notify consumers following a data breach have been defeated.[68] A better route to reform is through the Supreme Court accepting a "heightened risk of harm standard" for establishing standing, as this would resolve circuit splits in an expanding area of litigation in a way that both avoids the partisanship problem in Congress and accounts for the fact that the risk of identity theft is not speculative because criminals increasingly hack databases to sell stolen personal information or use it to commit other crimes.[69]

I. DEVELOPMENT OF STANDING DOCTRINE AND ITS APPLICATION TO DATA BREACH CASES

Article III standing, or the legal right to initiate a lawsuit, was articulated by the Supreme Court in *Lujan v. Defenders of Wildlife*.[70] There, the Court set forth three prongs to establish standing: (1) an "injury in fact," (2) a causal connection between the injury and the

---

[67] Thomas Martecchini, *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, 1494–95 (2016).

[68] *Id.*

[69] *See* Michael Hopkins, *Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches Not Sure" Should Not Be Enough to Put Someone in Jail for Life*, 50 U. PAC. L. REV. 427, 451 (2019).

[70] Lujan v. Defs. of Wildlife, 504 U.S. 555, 557 (1992) ("Environmental groups brought action challenging regulation of the Secretary of the Interior which required other agencies to confer with him under the Endangered Species Act only with respect to federally funded projects in the United States and on the high seas.").

lawsuit, and (3) the ability of a court to redress the issue.[71] The "injury in fact" prong was expressed by the Court to be an invasion of a legally protected interest which is (a) concrete and particularized and (b) "actual or imminent," not "conjectural" or "hypothetical."[72] The Court stated that the causal connection between the injury and the conduct complained of has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court."[73] To satisfy the third prong, "it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[74]

Clapper v. Amnesty International USA outlined the requirement of "actual or imminent" harm to establish standing.[75] In *Clapper*, plaintiffs challenged the Foreign Intelligence Surveillance ("FISA") Court Amendments Act of 2008, which permitted the FISA court (which oversees government requests for surveillance warrants against certain foreign agents) to authorize surveillance with no showing of probable cause that the target of the surveillance is an agent of a foreign power; the government need only show that the surveillance targets "persons reasonably believed to be located outside the United States" and seeks to "acquire foreign intelligence information."[76] Respondents ("United States persons [who claimed that they] engage[d] in sensitive international communications with individuals who they believe[d we]re likely targets of . . . surveillance")[77] alleged that the resulting highly permissive structure of electronic surveillance by the United States' National Security Agency on personal and private communications would cause them to suffer future injuries in the form of increased financial costs required to maintain confidentiality in overseas

---

[71] *Id.* at 560–62.

[72] *Id.* at 560.

[73] *Id.* at 560–61 (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41–42 (1976)).

[74] *Id.* at 561 (quoting *Simon*, 426 U.S. at 38, 43).

[75] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).

[76] *Id.* at 404–05.

[77] *Id.* at 401.

communications.[78] The Court dismissed the case on grounds that the challengers' claims that they were likely to be targets of surveillance were based "too much on a speculative chain of events that might never occur, and because an injury for the standing purposes must be 'certainly impending,' the plaintiffs could not satisfy the constitutional requirement for being allowed to sue."[79]

The Court found that "conjectural" injuries[80] that were neither "certainly impending" nor a "substantial risk" of creating future harm did not merit standing.[81] Justice Alito, writing for the majority, stated that "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[82] Noting the potential for government spying, however, four dissenting Justices stated that "[i]ndeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen."[83]

The decision in *Clapper*,[84] establishing that alleged harms must be "certainly impending," has been utilized as a defense by entities being sued for failing to adequately protect consumer data.[85] The "certainly impending" standard has proven an effective protection for breached entities because it is often difficult for consumers to connect the breach of information with a certainly impending harm.[86] Justice Breyer explained in his dissent in *Clapper* why

---

[78] *See id.* at 402, 406–07.

[79] ANDREW NOLAN, CONG. RESEARCH SERV., R43107, FOREIGN SURVEILLANCE AND THE FUTURE OF STANDING TO SUE POST-CLAPPER 7 (2013) (citing *Clapper*, 568 U.S. 413–14).

[80] City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1983) (describing conjectural injuries as injuries that lack immediacy and concreteness).

[81] *See Clapper*, 568 U.S. at 414–15 n.5.

[82] *Id.* at 416.

[83] *Id.* at 422 (Breyer J., Ginsburg J., Sotomayor J., Kagan J., dissenting).

[84] *Clapper*, 568 U.S. at 422.

[85] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 269 (4th Cir. 2017).

[86] *See* Sean McIntyre, *Deeper Dive: Clapper Divide Expands in Data Breach Cases*, DATA PRIVACY MONITOR (June 13, 2017), https://www.dataprivacymonitor.com/privacy-litigation/deeper-dive-clapper-divide-expands-in-data-breach-cases/.

plaintiffs struggle to make that connection when he critiqued the Court's use of a "certainly impending" standard:

> [T]he word "certainly" in the phrase "certainly impending" does not refer to absolute certainty. As our case law demonstrates, what the Constitution requires is something more akin to "reasonable probability" or "high probability." The use of some such standard is all that is necessary here to ensure the actual concrete injury that the Constitution demands.[87]

What Justice Breyer proposed is a standard more receptive of claims like those of data breach victims, who are largely unable to meet the "certainly impending" standard once their data is unauthorizedly accessed.

A. The Effect of Spokeo, Inc. v. Robins on Standing Doctrine

In 2016, the Supreme Court in *Spokeo, Inc. v. Robins* reiterated that in order to have Article III standing, the injury suffered must be "concrete *and* particularized."[88] In *Spokeo*, the plaintiff alleged that an internet search engine listed inaccurate information about his credit history in violation of the Fair Credit Reporting Act.[89] The Court held that the plaintiff's alleged reputational, intangible harm was not "concrete and particularized."[90] This would appear to weigh in favor of entities facing lawsuits related to data breaches in arguing that plaintiffs do not have Article III standing.[91] However, the Court failed to define what constitutes a "concrete" injury.[92] The portion of the *Spokeo* decision which established that an injury is "concrete" if there is a "risk of real harm"—as opposed to a purely statutory or

---

[87] *Clapper*, 568 U.S. at 440–41 (Breyer J., Ginsburg J., Sotomayor J., Kagan J., dissenting).

[88] Spokeo, Inc. v. Robbins, 136 S. Ct. 1540, 1545 (2016).

[89] *Id.* at 1544.

[90] *Id.*

[91] *See* LEBLANC & KNIGHT, *supra* note 62, at 1.

[92] *See generally* Spokeo, Inc. v. Robbins, 136 S. Ct. 1540 (2016) (failing to define a "concrete" injury in the context of standing doctrine).

abstract harm[93]—thus weighs in favor *plaintiffs* in data breach lawsuits attempting to establish standing to sue.

After *Spokeo*, the Third,[94] Sixth,[95] Seventh,[96] Eighth,[97] and the D.C Circuits[98] have been split with the Fourth[99] and Second[100] Circuits on what constitutes Article III standing in data breach lawsuits. The 2017 decisions in *Attias v. CareFirst, Inc.*, *Galaria v. Nationwide Mutual Insurance Co.*, and *In re SuperValu* illustrated that courts have become more inclined to find that Article III standing exists in class action data breach lawsuits.[101] However, inconsistency remains: the Third, Sixth, Seventh, and D.C. Circuits found standing even when the plaintiffs had suffered no monetary harm, whereas the Fourth and Second Circuits held that the plaintiffs did not have standing in similar circumstances.[102]

Spokeo's divergent progeny in the circuit courts with regard to stolen personal information[103] follows. In *Attias,* the D.C. Circuit reversed the district court's ruling that plaintiffs did not have standing when plaintiffs alleged that their health insurer failed to protect their personal information from a hack.[104] While there was no known misuse of the information, the D.C. Circuit found it

---

[93] *Id.* at 1549.

[94] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017).

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

[96] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

[97] *In re* SuperValu, Inc., 870 F.3d 766 (8th Cir. 2017).

[98] Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

[99] Beck v. McDonald, 848 F.3d 262, 274–75 (4th Cir. 2017).

[100] Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).

[101] *See* GIBSON, DUNN & CRUTCHER LLP, U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2018 21–22 (2018), https://www.gibsondunn.com/wp-content/uploads/2018/01/us-cybersecurity-and-data-privacy-outlook-and-review-2018.pdf.

[102] *Id.* at 22.

[103] *See generally* TRAVIS LEBLANC & KNIGHT, *supra* note 62 (analyzing how certain circuit courts have approved "several standing theories," whereas other circuits have not found standing in cases).

[104] Attias v. CareFirst, Inc., 865 F.3d 620, 622–23 (D.C. Cir. 2017) (Policyholders of CareFirst brought a class action suit against the insurer after personal information such as names, birthdates, email addresses, and subscriber identification numbers were stolen in a hack.).

plausible that the thieves who perpetuated the hack would misuse the personally identifiable information they had stolen.[105] The Seventh,[106] D.C.,[107] and Sixth[108] Circuits have all found that, when personal information is stolen, plaintiffs have standing based on the risk of a future harm because, as stated by the D.C. Circuit, "at the very least, it is plausible to infer that [the thief] has both the intent and the ability to use that data for ill."[109] Conversely, the Fourth Circuit did not find constitutional standing in *Beck v. McDonald* when a laptop with private information similar to the information in *Attias* was stolen, but the information was not misused.[110] There, the Fourth Circuit found that the risk to the plaintiffs was too speculative to find standing because it was not certain that the stolen information would be used for fraudulent purposes.[111] Similarly, in *Whalen v. Michaels Stores, Inc.*, the Second Circuit did not find standing when the details of the plaintiff's credit card were stolen by hackers who breached the defendant company's network.[112] The court found that there was no risk of future harm because the plaintiff had cancelled her credit card, eliminating the risk of harm in the court's perspective.[113]

The inconsistency among the circuits with respect to the theft of similar types of personal information[114] is particularly troublesome as data breaches become more common and as the market for stolen information continues to grow, making it harder for individuals to be aware that their information has been stolen until after misuse has

---

[105] *Id.* at 628.

[106] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).

[107] *See Attias.*, 865 F.3d at 620.

[108] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016).

[109] *Attias*, 865 F.3d at 628.

[110] *Compare id.*, *with* Beck v. McDonald, 848 F.3d 262, 277 (4th Cir. 2017) ("[N]ames, birth dates, the last four digits of social security numbers, and physical descriptors ([such as] age, race, gender, height, and weight)" were on the stolen laptops.).

[111] *Beck*, 848 F.3d at 274–76.

[112] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017).

[113] *Id.* at 90.

[114] *See In re* SuperValu, Inc., 870 F.3d 763, 773 (8th Cir. 2017); *Attias*, 865 F.3d at 629; *Whalen*, 689 F. App'x at 90–91; *Beck*, 848 F.3d at 267; Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016).

occurred. A "heightened risk of harm standard" would protect victims from a predominantly clandestine harm while not expanding standing doctrine problematically. Concerns for an expansive standing doctrine largely arise in lawsuits targeted at government action, coupled by complaints that expansion could busy the court system with matters that have legislative solutions rooted in the political process; this concern does not apply to legal action against private companies where the political process is not a realistic solution.[115]

B. The Effect of a Circuit Split on Standing in Data Breach Contexts

The lack of uniformity on the standing issue in data breach cases has substantial implications as more and more entities collect, aggregate, and use individuals' personal information. The vast collection of personal information creates a larger risk that the information will be misused, as a Pew survey found that 64% of Americans "have personally experienced a major data breach."[116] In 2019, a single data breach at Capital One caused over 100 million individuals to have their personal information—including bank accounts, social security numbers, names, addresses, and dates of birth—stolen.[117] The number of publicly reported data breaches leading to class action litigation continues to increase; "5.7% of data breaches publicly reported in 2018 led to class action litigation in 2018."[118] This is indicative of a potential increase in litigation

---

[115] Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 460 (2017).

[116] Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[117] Kelly Tyko, *Massive Data Breach Hits Capital One, Affecting More Than 100 Million Customers*, USA TODAY (July 29, 2019, 7:42 PM), https://www.usatoday.com/story/money/2019/07/29/capital-one-data-breach-2019-millions-affected-new-breach/1863259001/.

[118] ZETOONY ET AL., 2019 DATA BREACH LITIGATION REPORT, *supra* note 21, at 2 ("This is a 1.7% increase from 2017 and a 2.4% increase from 2016, indicating a steady increase in class action litigation relative to the number of breaches.").

nationwide if hackers continue to target personal information, chasing its increased value.[119]

As data breaches and data breach litigation alike become commonplace, a circuit split will continue to have disparate and detrimental effects on both entities that collect personal information and victims of data breaches. Inconsistency with regard to what types of harms establish standing will make it difficult for entities to evaluate the likelihood of data breach litigation and related costs.[120] Additionally, the victims of data breaches will continue to face uncertainty as to whether they have standing or if the courts will dismiss their efforts to be made whole for the pending threat of misused information and identity theft.[121] The current circuit split creates a legal environment wherein despite most entities collecting similar forms of personal information,[122] only victims of data breaches who decide to sue in favorable circuits are entitled to a remedy—a result that is neither fair nor just.

Different rulings on standing in data breach litigation have real impacts on the victims of data breaches. Once cases survive a motion to dismiss on standing grounds, they typically settle because data breaches attract regulatory attention and bad press for the breached entity: "negative reputational and branding impacts" of data breaches on the entities that could not protect personal information largely motivate decisions to settle.[123]

---

[119] *Id.* at 1 (noting "a 26% increase" in the number of class actions filed from 2016 to 2018 and a "100% increase" compared to the 2017 report).

[120] *See* Megan L. Brown et al., *D.C. Circuit Data Breach Standing Decision Will Encourage More Litigation Over Security in New Technology*, WILEY REIN LLP (Aug. 2017), https://www.wileyrein.com/newsroom-newsletters-item-PIF_August_2017-DC_Circuit_Data_Breach_Standing_Decision_Will_Encourage_More_Litigation_Over_Security_in_New_Technology.html.

[121] *See Do Data Breach Victims Have Standing to Sue?*, CONCORD L. SCH. (June 28, 2019), https://www.concordlawschool.edu/blog/news/do-data-breach-victims-have-standing-to-sue/.

[122] *See* Adam C. Uzialko, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (Aug. 3, 2018, 2:25 PM), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[123] Alexander H. Southwell et al., *Gibson Dunn Reviews U.S. Cybersecurity and Data Privacy*, COLUMBIA L. SCH. BLUE SKY BLOG (Feb. 3, 2017),

Defendants choosing to settle represent a widespread trend, as evidenced by settlements with consumer-plaintiffs, financial institution-plaintiffs, and attorney general-plaintiffs alike.[124] Large settlement agreements over data breaches included Anthem's $115 million settlement after hackers gained access to almost 80 million customer records;[125] Target's $18.5 million settlement after hackers obtained credit card, debit card, and personal information of fifty million customers;[126] and Home Depot's $25 million settlement after hackers stole customer payment information from self-checkout machines.[127] These multi-million-dollar settlement agreements indicate the need for entities possessing personal information to take measures to avoid and respond to lawsuits through both increased security measures and legal preparation for seemingly inevitable data breach lawsuits.[128] The ability to prepare for breaches and lawsuits, however, is conditioned upon an understanding of what plaintiffs can and cannot sue for—a concept currently non-uniform.

---

http://clsbluesky.law.columbia.edu/2017/02/03/gibson-dunn-reviews-u-s-cybersecurity-and-data-privacy/.

[124] David Balser et al., *Insight: Data Breach Litigation Trends to Watch,* BLOOMBERG L. (Mar. 4, 2019), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch.

[125] Aaron P. Bernstein, *Anthem to Pay Record $115M to Settle Lawsuits Over Data Breach*, NBC NEWS (Jun. 23, 2017, 6:41 PM), https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246.

[126] Sruthi Ramakriishnan & Nandita Bose et al., *Target in $18.5 Million Multi-State Settlement Over Data Breach*, REUTERS (May 23, 2017, 12:30 PM), https://www.reuters.com/article/us-target-cyber-settlement/target-in-18-5-million-multi-state-settlement-over-data-breach-idUSKBN18J2GH.

[127] Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, FORTUNE (Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks/.

[128] *See* Raymond Pompon, *Breach Costs Are Rising with the Prevalence of Lawsuits*, F5 LABS (May 2, 2018), https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits (listing the most recent settlement agreements in class action lawsuits with consumer-plaintiffs, financial institution-plaintiffs, and attorney general-plaintiffs).

II. FINDING THAT STANDING DOES NOT EXIST IN A DATA BREACH CONTEXT

Some circuits have maintained that Article III standing does not exist when a plaintiff only shows an increased risk of harm as a result of the subject data breach.[129] The lack of clarity in the Supreme Court decision in *Spokeo, Inc. v. Robins* has contributed to the Fourth and Second Circuits concluding that future harms cannot establish standing while other circuits have concluded the opposite, finding that future harm is enough to establish standing.[130]

A. The Fourth Circuit—A High Standard for Standing Unmet

The Fourth Circuit did not find constitutional standing in *Beck v. McDonald* when a laptop connected to a pulmonary functioning device and four boxes of pathology reports were misplaced or stolen from William Jennings Bryan Dorn Veterans Affairs Medical Center ("the VAMC") in Columbus, South Carolina.[131] The stolen or misplaced laptop contained unencrypted personal information of approximately 7,400 patients, and the boxes held information on over 2,000 patients.[132] The information included names, birth dates, the last four digits of social security numbers, descriptive traits of patients, and medical diagnoses.[133] Breaches similar to this are problematic because hackers typically use this type of information to open lines of credit or take out loans in patients' names.[134] The VAMC's internal investigation concluded that the laptop was likely stolen and that the stolen information was attributable to the VAMC's failure to follow proper procedures for maintaining

---

[129] LEBLANC & KNIGHT, *supra* note 62.

[130] *See id.* at 1, 3.

[131] Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).

[132] *Id.* at 267–68.

[133] *Id.* at 268. .

[134] *What Hackers Actually Do with Your Stolen Medical Records*, ADVISORY BOARD (Mar. 1, 2019, 10:00 AM), https://www.advisory.com/daily-briefing/2019/03/01/hackers.

personal information on encrypted computers.[135] The VAMC subsequently contacted patients whose personal information was stolen and notified them of the breach,[136] in accordance with South Carolina data breach notification requirements.[137] After litigation ensued, the VAMC suffered "at least seventeen [additional] data breaches" due to failure to implement proper procedures to secure information.[138]

Richard Beck and Lakreishia Jeffrey, veterans who received treatment at the VAMC,[139] filed a putative class action suit on behalf of the victims of the stolen personal information from the initial breach on the VAMC laptop.[140] The plaintiffs sought declaratory and monetary relief under the Privacy Act of 1974[141] for the threat of "current and future substantial harm from identity theft and other misuse of their [p]ersonal [i]nformation."[142] Additionally, Beverly Watson filed a putative class action suit on behalf of the victims of the stolen personal information contained in the pathology reports;[143] the plaintiffs in that lawsuit also sought declaratory and monetary damages for the threat of future and current harm from identity theft and other misuse of their personal information.[144] These claims were consolidated, and the Fourth Circuit addressed the defendant's motion to dismiss for lack of subject matter jurisdiction.[145] After reiterating the standards from *Clapper v. Amnesty International USA*, the court examined the claims for (1)

---

[135] *Beck*, 848 F.3d at 276; Haley Amster, Beck v. McDonald: *Standing Requirements in Consumer Data Breach Suits*, JURIS (May 2, 2017), http://dukeundergraduatelawmagazine.org/2017/05/02/beck-v-mcdonald-standing-requirements-in-consumer-data-breach-suits/.

[136] *Beck*, 848 F.3d at 267.

[137] S.C. CODE ANN. § 39-1-90 (2019).

[138] *Beck*, 848 F.3d at 268.

[139] *Id.* at 267.

[140] *Id.*

[141] *See generally* Records Maintained on Individuals, 5 U.S.C. § 552a (2018) (explaining that the Privacy Act governs the maintenance and disclosure of records by federal agencies).

[142] *Beck*, 848 F.3d at 267.

[143] *Id.* at 268.

[144] *Id.*

[145] *Id.* at 266, 270.

an injury in fact; (2) a traceable connection between the alleged injury in fact and the conduct of the defendant; and (3) whether the court could provide a remedy to the injury alleged by the plaintiffs.[146]

The court began its analysis with a determination of whether an injury in fact existed in *Beck*,[147] clarifying that, while a threat of an injury may qualify as an injury in fact, that standard only applies under certain circumstances.[148] Following *Clapper*, the injury in fact must not be premised on a "highly attenuated chain of possibilities" but an injury that is "certainly impending."[149] In *Beck,* the court applied these principles to the plaintiffs' allegations of "(1) the increased risk of future identity theft, and (2) the cost of protecting against [identity theft]."[150] The plaintiffs relied on previous opinions from the Sixth, Seventh, and Ninth Circuits to demonstrate instances where future risk of identity theft proved sufficient to a finding of the existence of an injury in fact such that Article III standing was found to be intact.[151]

The Fourth Circuit rejected the other circuits' opinions, distinguishing *Beck* from cases that found standing in the context of data breach lawsuits.[152] It contended that the injury in fact in circuits that found standing created a sufficiently imminent injury, whereas in *Beck*, the alleged injury was overly speculative.[153] The injuries suffered in *Beck* were considered too speculative because (1) there was no proof that the thief stole the laptop with the purpose of obtaining the personal information on the laptop; (2) there was no proof that the thief stole the pathology reports with the purpose of obtaining the personal information enclosed within them; and (3) a

---

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

[147] *Beck*, 848 F.3d 262 at 269–71.

[148] "[T]he Supreme Court has 'emphasized repeatedly,' an injury-in-fact 'must be concrete in both a qualitative and temporal sense.'" *Beck*, 848 F.3d at 271 (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)); Friends of Earth Inc., v. Gatson Cooper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000).

[149] *Beck*, 848 F.3d at 272 (quoting *Clapper*, 568 U.S. at 410).

[150] *Id.* at 273.

[151] *See id.* at 273–74.

[152] *See id.* at 274 (purporting to distinguish the facts at hand from other cases that found standing in data breach settings).

[153] *Id.*

substantial amount of time had passed without plaintiffs suffering a harm.[154]

The court in *Beck* determined that, in cases which found standing, the individual(s) who stole personal information acted with the sole purpose of obtaining stolen personal information.[155] The Fourth Circuit distinguished the facts in *Beck* when it concluded that there was a deliberate targeting of personal information in those other cases, and in so finding it relied upon factors including the sophistication of the hacking that took place, the lack of an alternative explanation for the hacking, and the fraudulent activity (such as identity theft and fraudulent charges) suffered by the plaintiffs.[156] In *Beck*, the absence of proof that the stolen laptop and pathology reports were opened or that the thief stole those items with the intention of obtaining personal information prevented the court from concluding that an injury in fact existed.[157] The VAMC's internal investigation determining the items were stolen as a result of theft was insufficient to confer standing because it did not demonstrate that the purpose of the theft was to obtain personal information.[158] Additionally, the alleged injuries were seen as speculative because no actual harm or fraudulent activity occurred in the two years following the theft.[159]

The analysis of whether there was a possible "injury in fact" in *Beck* continued with a determination of whether or not a "substantial risk" of harm existed.[160] The Fourth Circuit rejected statistics showing that data breaches result in identity theft as well as the VAMC's offer of free credit monitoring to plaintiffs as evidence of a "substantial risk."[161] Additionally, the court refused to conclude

---

[154] *Id.* at 274–75.

[155] *See id.* at 273.

[156] *Id.* at 273 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694–95 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632–34 (7th Cir. 2007)).

[157] *Beck*, 848 F.3d at 275.

[158] *Id.* at 267, 275.

[159] *Id.* at 274.

[160] *Id.* at 276.

[161] *Id.* at 268.

that the purchase of credit monitoring software and the burden of monitoring personal accounts for fraud constituted an injury in fact.[162] Although the risk of future harm through identity theft could constitute a "substantial" harm, the court concluded the threat was self-imposed and "speculative" because it was not certainly impending and therefore did not merit finding standing.[163]

B. The Second Circuit—One Fraudulent Credit Card Charge is Insufficient to Find Standing

Courts have been unwilling to clarify how extensive the harm suffered by a plaintiff must be to satisfy the injury in fact prong of standing analysis. In *Whalen v. Michaels Stores, Inc.*, the Second Circuit examined a case where the plaintiff's credit card information was stolen during the course of a data breach at Michaels Stores.[164] After the breach, Michaels Stores issued a press release stating that customers' credit and debit card information was stolen in a breach and that Michaels would be offering twelve months of identity protection and credit card monitoring services to customers for free.[165] The plaintiff alleged that "(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 [] lost time and money resolving the attempted fraudulent charges and monitoring her credit."[166]

As in *Beck*,[167] the court in *Whalen* did not find that an injury in fact occurred; therefore, Article III standing did not exist.[168] The plaintiff was neither "asked to pay, nor did [she] pay [for,] any [of the] fraudulent charge[s]" because the credit card was cancelled before the plaintiff became liable for any charges.[169] That fact that the charges were fraudulently made was not "particularized and

---

[162] *Id.*

[163] *Id.* at 276–77 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013)).

[164] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

[165] *Id.*

[166] *Id.*

[167] *Beck*, 848 F.3d at 276.

[168] *Whalen*, 689 F. App'x. at 91.

[169] *Id.* at 90.

concrete" enough for the court to find standing because she did not suffer any monetary losses, nor did she face any future threat of monetary loss.[170] Additionally, because no other personally identifiable information was stolen from Michaels Stores, there was no future risk of identity theft.[171] The court found that the plaintiff's claim that she spent additional time and money monitoring her account in response to potential fraudulent activity was insufficiently supported with regard to the efforts undertaken to show an injury in fact.[172]

III. FINDING STANDING IN A DATA BREACH CONTEXT

While some circuits have maintained that Article III standing does not exist as a result of an increased risk of harm in a data breach context,[173] others have found standing based on various theories.[174] The Eighth Circuit found standing based on de minimis harm, and the Third Circuit found an injury based on a statutory violation.[175] Additionally, the D.C., Sixth, and Seventh Circuits have found standing based on the substantial risk of harm created during a data breach.[176] These circuits demonstrate drastic divergence amongst the courts with regard to their interpretation of the standing doctrine in the data breach context, even when the ultimate result is a finding of standing.

---

[170] *Id.*

[171] *Id.*

[172] *Id.* at 91.

[173] *See id.*; Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017).

[174] *See In re* SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017); Attias v. CareFirst Inc., 865 F.3d 620, 628 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

[175] *In re SuperValu, Inc.*, 870 F.3d at 773; *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 631 (3d Cir. 2017); LEBLANC & KNIGHT, *supra* note 62, at 2.

[176] *See Attias*, 865 F.3d at 628; *Galaria*, 663 F. App'x at 388; *Remijas*, 794 F.3d at 690.

A. Article III Standing Based on De Minimis Harm

In *In re SuperValu, Inc.,* the Eighth Circuit found standing in a manner that, at least facially, appeared to conflict with the decisions in the Fourth and Second Circuits.[177] Similar to the facts in *Whalen v. Michaels Stores, Inc.*,[178] the hackers in *SuperValu* installed malware in the network of SuperValu grocery stores in order to access records of consumer credit card transactions.[179] As in *Whalen*, the information stolen by hackers was limited to credit card numbers, expiration dates, and card value verification codes.[180] The plaintiffs alleged that hackers accessed their information because of SuperValu's poor security measures.[181] These alleged inadequacies included easy-to-guess and unencrypted passwords meant to protect sensitive information, failure to segregate credit card information from other parts of the company's network, and the absence of protective firewalls.[182] The plaintiffs in *SuperValu* alleged that, as a result of the security breach, they faced an imminent threat of identity theft, sacrificed time monitoring accounts to ensure there was no fraudulent activity, and awaited the constant possibility that their credit card information would be used for prolonged periods of time to perpetuate fraudulent activity.[183] They attempted to support their claims with a Government Accountability Office report on the likelihood of identity theft as a result of a data breach.[184]

The plaintiffs in *SuperValu* alleged that inadequate security measures allowed for a breach that caused the same injury in fact as

---

[177] *In re SuperValu*, *Inc*., 870 F.3d at 773 (finding that plaintiff had Article III standing based on one instance of unreimbursed fraudulent credit card activity). *But cf. Whalen*, 689 F. App'x at 91; *Beck*, 848 F.3d at 277–78.

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

[179] *In re SuperValu*, *Inc.*, 870 F.3d at 766.

[180] *Id.*

[181] *Id.* at 770.

[182] *Id.* at 766.

[183] *Id.* at 766–67.

[184] The Government Accountability Office "examines the use of public funds; evaluates federal programs and activities; and provides analyses, options, recommendations, and other assistance to help the Congress make effective oversight, policy, and funding decisions." *GAO's Mission, Responsibilities, Strategies, and Means*, GAO U.S. GOV'T ACCOUNTABILITY OFF., https://www.gao.gov/dsp/3mission.html (last visited Sept. 18, 2019).

in *Whalen*—fraudulent credit card charges as a result of stolen credit card information.[185] In *Whalen*, the plaintiff brought a class action suit based on claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of various state consumer protection and data breach notification laws.[186] In *SuperValu*, the Eighth Circuit dismissed the claims brought by all of the plaintiffs except for one, the plaintiff who had incurred a fraudulent charge.[187] The complaint in *Whalen* "assert[ed] claims for breach of an implied contract and for a violation of New York General Business Law [Section] 349."[188] In both cases, plaintiffs attempted to bolster the existence of an injury in fact by providing statistics on the likelihood that their personal information would be used for criminal activity as a result of data breaches.[189] Additionally, the defendants in both cases issued similar press releases informing the public that a theft of consumer information occurred.[190]

In *SuperValu*, the Eighth Circuit began its analysis by conducting an injury in fact analysis on the plaintiffs whose credit card information had not actually been misused to ascertain if they had standing to sue and could therefore survive defendants' motion to dismiss.[191] In applying the standards established in *Clapper v. Amnesty International USA*, the court concluded that for these plaintiffs, the alleged injury was too speculative to find that Article III standing existed.[192] In coming to this conclusion, the court rejected the assertion that, based upon information and belief, plaintiffs' information was being sold on websites and their respective financial institutions were undertaking a heavy burden to protect their information.[193] Similar to *Beck v. McDonald*, the court in *SuperValu* rejected the contention that statistics indicating an increased likelihood of theft after a data breach were sufficient to

---

[185] *In re SuperValu, Inc.*, 870 F.3d at 766.

[186] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

[187] *In re SuperValu, Inc.*, 870 F.3d at 775.

[188] *Whalen*, 689 F. App'x at 89.

[189] *In re SuperValu, Inc.*, 870 F.3d at 767; *Whalen*, 689 F. App'x at 90.

[190] *In re SuperValu, Inc.*, 870 F.3d at 766; *Whalen*, 689 F. App'x at 90.

[191] *In re SuperValu, Inc.*, 870 F.3d at 768.

[192] *Id.* at 769–72.

[193] *Id.* at 770.

prove that a "substantial risk of future identity theft" existed; it held that the complaint did not sufficiently allege a substantial risk of identity theft and that the customers' allegations of future injury did not support standing.[194] In light of this, the court granted the defendants' motion to dismiss for all plaintiffs who did not incur a fraudulent charge, but it found that standing existed for the sole plaintiff whose credit card incurred a fraudulent charge because the complaint contained sufficient allegations to demonstrate that the customer "suffered an injury in fact, fairly traceable to the defendants' security practices, and likely to be redressed by a favorable judgment."[195]

The court in *SuperValu* concluded that a fraudulent charge is a form of identity theft that constitutes a "concrete[] and particularized injury" which satisfies the injury in fact requirement for Article III standing.[196] This is in stark contrast with the decision of the Second Circuit in *Whalen*, where the court found that a fraudulent credit card charge did not constitute a "particularized and concrete" injury because the company cancelled the credit card without the plaintiff being held liable for the charges.[197] Despite an abundance of factual similarities, *SuperValu* and *Whalen* came to opposite conclusions.[198] Both cases involved hackers gaining access to a network of consumers' credit card information, and both breaches resulted in a fraudulent charge against a plaintiff.[199] Furthermore, the data breaches in both cases did not involve personal information beyond the scope of stolen credit card information.[200] But similar factual situations have proven insufficient for consistency in this respect.

The differing conclusions are at least partially attributable to the Eighth Circuit finding the burden of establishing standing to be a

---

[194] *Id.* at 771–72.

[195] *Id.* at 773.

[196] *Id.* at 770.

[197] Whalen v. Michaels Stores, Inc., 689 F. App'x. 89, 90–91 (2d Cir. 2017).

[198] *See In re SuperValu*, *Inc.*, 870 F.3d at 774; *Whalen*, 689 F. App'x at 90–91.

[199] *See In re SuperValu, Inc.*, 870 F.3d at 767; *Whalen*, 689 F. App'x at 90.

[200] *See id.*

"threshold inquiry."[201] The "threshold inquiry" standard enabled the Eighth Circuit to find that incurring fraudulent charges satisfied the "general allegations" necessary to establish an injury in fact—regardless of whether the charges were reimbursed or not.[202] This analysis directly contradicts the value the Second Circuit placed on whether the fraudulent charges were reimbursed in *Whalen*: the Eighth Circuit concluded reimbursement did not quash the injury in fact prong, but the Second Circuit found that reimbursed fraudulent charges did not constitute an injury in fact.[203] The court did not need to reach the possibility of a future harm satisfying the injury in fact prong in an Article III standing analysis because it found that incurring fraudulent charges, regardless of reimbursement, constituted an injury in fact.[204] The seemingly arbitrary distinction in the injury in fact analysis between the Second and Eighth Circuits adds to the unpredictability in data breach standing doctrine regarding whether victims of data breaches have standing when charges are reimbursed.[205]

The Eighth Circuit in *SuperValu* continued its standing analysis by applying the remaining two factors necessitated by *Clapper*: (1) that a causal connection between the injury suffered and the alleged wrongful conduct exists, and (2) that a court can redress the injury.[206] The analysis turned to the causation between the alleged injury in fact, the fraudulent charges, and the breach of SuperValu's network.[207] The court rejected the defendants' argument that the plaintiff must allege his particular fraudulent charge was a result of the defendants' data breach.[208] Instead, the court required that he allege his fraudulent charge was fairly traceable to the defendants'

---

[201] *In re SuperValu, Inc.*, 870 F.3d at 773. "[S]tanding under Article III presents only a 'threshold inquiry,' requiring 'general allegations' of injury, causation, and redressability." *Id.* (citations omitted).

[202] *Id.*

[203] *In re SuperValu, Inc.*, 870 F.3d at 774; *Whalen*, 689 F. App'x at 90 (concluding that because the plaintiff was neither asked to pay nor did she pay for any of the fraudulent charges, no injury in fact occurred).

[204] *In re SuperValu, Inc.*, 870 F.3d at 773.

[205] *See In re SuperValu, Inc.*, 870 F.3d at 767; *Whalen*, 689 F. App'x at 90.

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

[207] *See In re SuperValu, Inc.*, 870 F.3d at 772.

[208] *Id.*

breaches.[209] Plaintiff's statement of a causal connection between the deficiencies and failures in the defendants' cybersecurity, the hacking of the defendants' network, the theft of customers' credit card information from defendants' network, and the plaintiff's incurring a fraudulent credit card charge satisfied the causation requirement of the court's standing analysis.[210] Lastly, the court concluded it had the power of redressability as it applied to the unreimbursed fraudulent charges.[211] The Eighth Circuit finding that plaintiffs have standing from one potentially reimbursed charge[212] creates an unequal application of standing doctrine and uncertainty for both victims of data breaches and entities responsible for personal information.

B. Article III Standing Based on a Statutory Violation

In Third Circuit case *In re Horizon Healthcare Services Inc. Data Breach Litigation*, two unencrypted laptops containing detailed personal information on approximately 839,000 clients were stolen from Horizon's headquarters.[213] The stolen laptops contained personally identifiable information and protected health information of clients and potential clients.[214] When the Horizon Healthcare clients filed suit, the Third Circuit found standing based on a violation of the Fair Credit Reporting Act ("FCRA").[215] The plaintiffs alleged that Horizon willfully and negligently violated the FCRA,[216] which attempts to protect consumer privacy and specifically imposes requirements on a "consumer reporting agency" that "regularly . . . assembl[es] or evaluat[es] consumer credit information . . . for the purpose of furnishing consumer reports to third parties."[217] The plaintiffs argued that Horizon

---

[209] *Id.*

[210] *Id.*

[211] *Id.* at 773.

[212] *See id.* at 774.

[213] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).

[214] *Id.*

[215] *Id.* at 635.

[216] *Id.* at 629.

[217] Definitions; rules of construction, 15 U.S.C § 1681a(f) (2018).

violated its statutory obligation when it failed to secure their information from unauthorized use, thereby constituting an injury in fact.[218]

The Third Circuit found that Congress may "cast the standing net broadly" and that a violation of a statutory right, even "absent evidence of actual monetary loss," can be sufficient to constitute an "actual or threatened injury."[219] The court explained that the violation of a statutory right creates a *de facto* injury that does not require focus on monetary losses.[220] The Third Circuit clarified that its ruling did not contradict the Supreme Court in *Spokeo* but followed *stare decisis* by concluding that the plaintiffs did suffer a "concrete" injury in *Horizon Healthcare*.[221] It reasoned that the plaintiffs alleged more than a "mere technical or procedural violation," but an "unauthorized dissemination of their own private information—the very injury that FCRA is intended to prevent."[222] The *Horizon Healthcare* decision provided another avenue—a violation of a statutory right—for plaintiffs in class action data breach lawsuits to obtain standing.[223] This route may increase the number of plaintiffs able to obtain standing, as new plaintiffs may seek to state claims based on the *Horizon Healthcare* precedent that a failure to protect personal information constitutes an injury in fact regardless of whether the plaintiffs suffered actual harm,[224] as plaintiffs who ground their standing on a statutory right do not need to prove that the stolen information caused them to suffer identity theft of any kind.[225]

---

[218] *See Horizon Healthcare*, 846 F.3d at 631–32.

[219] *Id.* at 635–36 (citations omitted).

[220] *See id.* at 636.

[221] *Horizon Healthcare*, 846 F.3d at 640; *see* Spokeo, Inc. v. Robbins, 136 S. Ct. 1540, 1550 (2016).

[222] *Horizon Healthcare*, 846 F.3d at 640.

[223] *Id.* at 640.

[224] Gregory N. Blasé et al., *Third Circuit Moves Toward a Broader View of Standing in FCRA Data Breach Class Action*, KL GATES (Jan. 30, 2017), http://www.klgates.com/third-circuit-moves-toward-a-broader-view-of-standing-in-fcra-data-breach-class-action-01-30-2017/.

[225] *Horizon Healthcare*, 846 F.3d at 640–41.

C. Standing Based on a Future Risk of Harm

Courts have varied with regard to what constitutes a future risk of harm,[226] further muddying the waters of standing doctrine. In *Clapper*, the Supreme Court held that the risk of future harm may satisfy the injury in fact requirement for Article III standing so long as the alleged harm is "certainly impending."[227] While the Fourth and Second Circuits found a plaintiff's risk of future harm in a data breach context too speculative to constitute an "injury in fact,"[228] the D.C., Sixth, and Seventh Circuits found that a future risk of harm does constitute an "injury in fact."[229] Satisfying the "injury in fact" prong is a considerable hurdle to achieving standing and marks a clear circuit split.[230] The more expansive approach to standing that considers a plaintiff's risk of future harm sufficient to constitute an "injury in fact" better values the intrusive nature of personal data disclosures and the ability to provide a remedy to an increasingly problematic topic.[231]

i. The D.C. Circuit

In *Attias v. CareFirst, Inc.*, healthcare provider CareFirst "failed to properly encrypt" its servers.[232] A breach occurred in 2014, resulting in the theft of an estimated one million insureds' personal information.[233] Seven insureds subsequently filed a class action

---

[226] Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388, (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).

[227] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

[228] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017).

[229] *Attias*, 865 F.3d at 623; *Galaria*, 663 F. App'x at 387–89; *Remijas*, 794 F.3d at 690.

[230] *Attias*, 865 F.3d at 627; *Galaria*, 663 F. App'x at 388; Remijas, 794 F.3d at 693–94.

[231] *See* Kelsey Harclerode, *Privacy, Mass Intrusion and the Modern Data Breach*, 69 FLA. L. REV. 771, 828 (2018).

[232] *Attias*, 865 F.3d at 623.

[233] *Id.* at 622.

lawsuit against CareFirst.[234] The parties disagreed on whether the hackers were able to obtain the insureds' social security numbers, and CareFirst sought to dismiss the claims for lack of standing.[235] Focusing on the "injury in fact" analysis, the court relied on *Clapper* to conclude that an "injury in fact" exists when there is a '"substantial risk' that the harm will occur."[236] Unlike in *Clapper*, however, the court concluded that there were not so many links in the causal chain as to make the alleged injuries too speculative; thus, the plaintiffs had standing.[237] This directly contradicts the decision in *Beck*, where the Fourth Circuit, applying *Clapper*, found that the theft of unencrypted laptops and pathology reports containing similar personal information was too speculative to confer standing without proof that the thief acted for the purpose of obtaining personal information.[238] Conversely, the court in *Attias* stated that, in assuming all the allegations in the complaint were true (meaning social security numbers and credit card information were stolen), it was not too speculative to consider the plausible harms that plaintiffs could endure because, "at the very least, it is plausible []to infer that [the thief] has both the intent and the ability to use that data for ill."[239] Moreover, the court reasoned that the nature of the hack and the information stolen merited a finding that a "substantial risk" existed.[240] Additionally, the court in *Beck* emphasized that, because the plaintiffs' stolen information was not used for fraudulent activity from the time of the theft in 2014 to the time of the suit in 2017, there was no risk of "substantial harm."[241] While the hack in *Attias* also occurred in 2014, the D.C. Circuit reasoned that the stolen information still created a plausible "substantial risk" of harm, irrespective of the time that had passed without incident such that the passage of time did not mitigate or negate the substantial risk.[242]

---

234 *Id.* at 623.

235 *Id.*

236 *Id.* at 626.

237 *Id.* at 629.

238 Beck v. McDonald, 848 F.3d 262, 274–75 (4th Cir. 2017).

239 *Attias*, 865 F.3d at 628.

240 *Id.* at 628.

241 *See Beck*, 848 F.3d at 275.

242 *See Attias*, 865 F.3d at 629.

ii. The Sixth Circuit

In *Galaria v. Nationwide Mutual Insurance Co.*, financial and insurance company Nationwide suffered a personal network hack.[243] The breached network held the names, dates of birth, employment histories, and social security numbers of over 1.1 million customers.[244] Following the breach, the victims filed a class action suit against Nationwide alleging FCRA violations and additional claims based on negligence, invasion of privacy by public disclosure of private facts, and bailment.[245] Just as in *Beck* and *Whalen*, the plaintiffs in *Galaria* alleged that the theft left them with an increased risk of identity theft and that as a result they would incur "financial and temporal" losses.[246] The court did not find standing based on the alleged FCRA violation as in *Horizon Healthcare*[247] but instead focused on the "substantial risk" of harm to the victims of the data breach.[248]

Similar to *Attias*, the court in *Galaria* found that the theft of the personal information created a substantial risk in and of itself.[249] This decision to find a "substantial risk" of harm solely based on the theft of personal information differs from the courts in *Beck* and *Whalen*, which found that theft of information alone was too speculative to confer standing.[250] While the court in *Beck* refused to find that the defendant offering to pay for credit monitoring services was evidence of a "substantial risk," the court in *Galaria* came to the opposite conclusion when it stated, "Nationwide seems to recognize the severity of the risk, given its offer to provide credit-

---

[243] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016).

[244] *Id.* at 387–89.

[245] *Id.*

[246] *Id.* at 386, 388.

[247] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 640 (3d Cir. 2017).

[248] *Id.* at 387–88.

[249] Attias v. CareFirst Inc., 865 F.3d 620, 628 (D.C. Cir. 2017); *Galaria*, 663 F. App'x at 388 (6th Cir. 2016).

[250] *See* Galaria, 663 F. App'x at 387–89. *But see* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

monitoring and identity-theft protection for a full year."[251] Additionally, the Sixth Circuit in *Galaria* stated that any time and money the plaintiffs spent monitoring their credit, checking their bank statements, or modifying their financial accounts constituted "an actual injury."[252] While the court in *Whalen* found that the lack of specificity in the allegations that the data breach caused the plaintiff to expend time and money monitoring credit or checking bank statements, the decision in *Galaria* makes it possible for specifically-pleaded allegations to merit the court's finding of an "actual injury."[253] The Seventh Circuit and the D.C. Circuit followed and supported the Sixth Circuit's conclusion that courts need not wait for actual misuse to occur to establish standing.[254]

iii. The Seventh Circuit

In *Remijas v. Neiman Marcus Group, LLC*, hackers obtained the credit card information of consumers through malware installed on Neiman Marcus department store servers.[255] The hackers obtained nearly 350,000 credit card numbers, and 9,200 of those cards affirmatively reported fraudulent activity.[256] The plaintiffs filed a class action lawsuit alleging negligence, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of multiple state data breach laws.[257] Just as in *Whalen* and *Beck*, the plaintiffs in *Remijas* filed suit based on "lost time and money protecting themselves against future identity theft."[258]

In analyzing the plaintiffs' standing, the court in *Remijas* turned to the *Clapper* standard and looked to determine whether an injury

---

[251] *Beck*, 848 F.3d at 276 n.8; *Galaria*, 663 F. App'x. 384, 388 (6th Cir. 2016).

[252] *Galaria*, 663 F. App'x 384, 387–90.

[253] *Whalen*, 689 F. App'x at 90; *Galaria*, 663 F. App'x at 390.

[254] *See* Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

[255] *Remijas*, 794 F.3d at 690.

[256] *Id.*

[257] *Id.* at 690–91.

[258] *Compare* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017), and Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017), *with Remijas*, 794 F.3d at 692.

in fact had occurred.[259] Just as in *Whalen*, the plaintiffs in *Remijas* argued that they suffered lost time and money spent "replacing cards and monitoring their credit score[s]."[260] Unlike in *Beck*, the Seventh Circuit found that (1) the theft of personal information alone was not too speculative to create a "substantial risk" of harm because of the "objectively reasonable likelihood" that harm will occur, and (2) plaintiffs did not have to wait for the harm to occur to have standing.[261] This differs from the Fourth Circuit's finding in *Beck* that (1) the theft of an unencrypted laptop and pathology reports containing personal information was too speculative to conclude the thieves intended to use the information, and that (2) because no harm occurred, the plaintiffs were not at risk of fraud or identity theft.[262] The court's finding of an "injury in fact" in *Remijas*—where fraudulent credit card charges were reimbursed[263]—also directly contrasts with the Third Circuit's finding in *Whalen* that an "injury in fact" did not occur when fraudulent credit card charges were reimbursed by the issuing credit card company.[264] This inconsistency leaves plaintiffs involved in data breach litigation increasingly uncertain as to whether they have standing until the Supreme Court effectuates a uniform application of standing doctrine.

IV. A SOLUTION TO THE CIRCUIT SPLIT ON DATA BREACH LITIGATION—RISK OF FUTURE HARM CREATES STANDING

The status of standing in data breach litigation is currently split into three branches, where: (1) risk of a future harm does not create standing;[265] (2) risk of a future harm does create standing;[266] or (3)

---

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

[260] *Whalen*, 689 F. App'x at 90; *Remijas*, 794 F.3d at 692.

[261] *Remijas*, 794 F.3d at 693 (quoting *Clapper*, 568 U.S. at 410).

[262] *Beck*, 848 F.3d at 275.

[263] *Remijas*, 794 F.3d at 696–97.

[264] *Whalen*, 689 F. App'x at 90–91.

[265] *See id.* at 89; *Beck*, 848 F.3d at 267.

[266] Attias v. CareFirst Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–89 (6th Cir. 2016); *Remijas*, 794 F.3d at 661.

a statutory violation creates standing regardless of whether harm actually occurred.[267] Standing interpretation in data breach litigation should be narrowed into the two branches that do not contradict each other, such that: (1) risk of a future harm does create standing, and (2) a statutory violation creates standing regardless of whether harm actually occurred. Creation of this bifurcation where both theories can coexist would enable more plaintiffs to seek a remedy for the theft of their personal information. It would also encourage entities that maintain sensitive information to increase security because they would face more accountability as an increasing number of data breach lawsuits would survive motions to dismiss and reach judgments on the merits.[268]

A. Justice and Accountability: Increased Risk of Future Harm Creates Standing

The Second and Fourth Circuits' interpretations that the risk of future harm does not create standing[269] differs from the D.C., Seventh, Eighth, and Ninth Circuits' understanding that the risk of future harm may confer standing.[270] To reiterate, the standing requirements, as articulated in *Clapper*, are that there be: (1) an injury in fact, (2) redressability, and (3) a causal connection between the injury in fact and the matter brought into court.[271] Interpreting the standing doctrine to require only a "reasonable likelihood" that information will be used for fraudulent purposes (as opposed to

---

[267] *See In re* SuperValu, Inc., 870 F.3d 763, 767, 773 (8th Cir. 2017).

[268] *See* LEBLANC & KNIGHT, *supra* note 62, at 1.

[269] *See generally* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (noting that absent any evidence to indicate a plaintiff may "plausibly face a threat of future [harm]," the plaintiff suffers no injury and thus cannot satisfy the standing requirement); *Beck*, 848 F.3d at 272 (discussing how absent any evidence that risk of future harm "was certainly impending," plaintiffs cannot satisfy the standing requirement).

[270] *Attias*, 865 F.3d at 622 (finding that risk of future harm was not "too speculative" to constitute an injury in fact to meet the standing requirement); *Galaria*, 663 F. App'x at 385 (determining the plaintiffs had Article III standing partially because such theft placed them at a continuing risk of harm); *Remijas*, 794 F.3d at 692 (holding that if an allegation of future harm is "certainly impending," the allegation may establish standing).

[271] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

waiting for fraudulent activity to occur) satisfies the "actual or imminent" prong, and in the same way, finding that taking measures after falling victim to a data breach satisfies the "concrete and particularized" prong would help resolve the conflicting opinions among the circuits and give both victims and information-holding entities predictability.[272]

i. Injury in Fact

Many of these circuits arrived at differing conclusions because of the competing analysis of what constitutes an injury in fact.[273] As explained in *Lujan v. Defenders of Wildlife*, an injury in fact is a harm that is "concrete and particularized" and "actual or imminent," not "conjectural or hypothetical."[274] Applied to the data breach context, courts have proven unable to decide whether the theft of personal information is an injury in fact or whether victims of a breach must wait until that stolen information is used to their detriment.[275] Data breach cases often involve harms that have not yet occurred, and so the determination that the harms are "actual or imminent" is generally established by a showing that there is a substantial risk of injury to the plaintiffs.[276]

a. "Actual or Imminent"

An alleged harm is "actual or imminent" if there is a substantial risk that the harm will occur.[277] Courts should consider the "reasonable likelihood" that the breached information will be used for fraudulent purposes as opposed to waiting for victims to experience fraudulent activity. It should not be necessary for

---

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

[273] *In re* SuperValu, Inc., 870 F.3d 763, 773–74 (8th Cir. 2017); *Attias*, 865 F.3d at 629; *Whalen*, 689 F. App'x at 90; *Beck*, 848 F.3d at 272; *Galaria*, 663 F. App'x at 387–89.

[274] *Lujan*, 504 U.S. at 560.

[275] Spinelli*, supra* note 37.

[276] *See Attias*, 865 F.3d at 629; *Beck*, 848 F.3d at 276; *Galaria*, 663 F. App'x at 388–89; Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

[277] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 412 (2013).

plaintiffs to demonstrate that the thief or hacker stole personal information for the purposes of fraudulent activity to create a substantial risk of harm; "why else would hackers break into a store's database and steal personal information?"[278] Additionally, defendants offering to pay for credit monitoring services should be considered an indication that a substantial risk of harm exists.[279] These interpretations of the "actual or imminent" prong of the injury in fact analysis would create a uniform result that would reduce barriers to recovery for legitimate injuries in fact.[280]

If the Fourth Circuit in *Beck* followed this analysis, the court likely would not have required the plaintiffs to indicate that the thieves stole the unencrypted laptop and pathology reports for the personal information within them because it would have recognized that information is inherently valuable, creating an obvious target.[281] In applying the solution proposed in this Note, theft of patients' personal information in cases like *Beck*[282] would create a reasonable likelihood that the information would be used for fraudulent purposes since it was taken by illegal means. Additionally, the offering of one year of credit monitoring to victims of the breach would be an indication that "a substantial risk" of fraudulent activity exists.[283] If the proposed analysis were applied in *Whalen*, instead of concluding the injuries suffered were not actual, the court could have concluded that the plaintiffs incurred the actual injury of monitoring fraudulent activity on accounts and being at risk of the

---

[278] *Remijas*, 794 F.3d at 693.

[279] Martecchini, *supra* note 67, at 1492.

[280] *See id.* (The author proposes an alternative framework to avoid "inconsistent results depending on the court" and suggests that an improvement to "the data-breach standing analysis is necessary.").

[281] *See* Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017) (requiring the plaintiffs to demonstrate that hackers stole the laptop and pathology reports for misuse of personal information).

[282] *Id.*

[283] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690–93 (7th Cir. 2015) ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach.").

future risk of identity fraud, as thieves often open new credit cards without people's knowledge.[284]

b. "Concrete and Particularized"

An injury is considered "particularized" when it affects the plaintiff "in a personal and individual way."[285] There is little debate that when a plaintiff's personal information is stolen it directly harms the plaintiff (as opposed to a third party or the public).[286] An injury is considered "concrete" when it involves something "real"—such as money—as opposed to something abstract.[287] In *Schlesinger v. Reservists Committee to Stop the War*, the Supreme Court considered the claim that the government's failure to comply with the Incompatibility Clause (which prohibits a person from simultaneously holding offices in both the executive and legislative branches of the federal government) would only affect the "generalized interest of all citizens in constitutional governance" to be abstract because the plaintiffs did not suffer a harm particular to the action.[288] The actions individuals must take following a breach of their personal information—such as purchasing credit-monitoring services, replacing credit cards, monitoring financial statements, ordering new checks, and buying identity theft insurance—should qualify as a "concrete injury" if they are sufficiently specific.[289] The interpretation of the "concrete" injury requirement in *Schlesinge*r that requires sufficiently specific actions to be taken following a breach of personal information would have likely been satisfied by the plaintiffs in *Beck*, as opposed to being seen as an effort to mitigate future harm, when they obtained credit

---

[284] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017); *Remijas*, 794 F.3d at 693–94 (A showing of "actual" injury must be made for the purposes of Article III standing; the court noted that the mitigation expenses alone did not qualify as actual injuries sufficient for standing.).

[285] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 n.1 (1992).

[286] *See* Spokeo, Inc. v. Robbins, 136 S. Ct. 1540, 1548 (2016).

[287] *Id.* at 1548.

[288] Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 210, 217 (1974).

[289] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).

monitoring software after the theft of their personal information.[290] Additionally, this likely would have created a "concrete" injury for the plaintiff in *Whalen* had she provided specific expenses and detailed the effort she underwent after the theft of her information instead of being overly vague.[291] This analysis requiring simply that an injury in fact not be vague likely would have enabled the court in *SuperValu* to find standing regardless of whether a fraudulent charge was incurred because the specific time and effort spent protecting and monitoring the victims' accounts likely would have been sufficiently concrete.[292] In addition to a disregard of time, effort, and expense as non-abstract, requiring plaintiffs to wait for fraudulent activity is problematic and unjust because the more time that passes between a data breach and an instance of identity theft, the easier it is for the defendant to argue that the fraudulent activity is not "fairly traceable" to the defendant's data breach.[293] The proposed standard is an application of standing doctrine that adequately responds to the modern dilemma of data breaches.

c. Redressability and a Causal Connection

The next standing requirement—redressability—is easily demonstrated under the suggested interpretation of the standing doctrine. The "concrete" harm of purchasing credit-monitoring services, replacing credit cards, monitoring financial statements, ordering new checks, and buying identity theft insurance is redressed by a favorable verdict that grants compensatory damages.[294] The final requirement for standing—that the alleged injuries be "fairly [ ] trace[able]" to the defendant[295]—does not require that the defendant be the immediate cause of the data breach (through inadequate security or another failure), only that the

---

[290] Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017).

[291] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

[292] *In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017).

[293] *Id.*

[294] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390–91 (6th Cir. 2016).

[295] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41–42 (1976)).

injuries be fairly traceable.[296] Courts have found that defendants being one step removed from hackers still have a fairly traceable connection to alleged injuries.[297]

B. If It Ain't Broke, Don't Fix It: Standing Based on a Statutory Violation

Congress' power to create statutes and give individuals the ability to enforce their individual rights is not a new concept but a well-established practice related to the standing doctrine.[298] An application of standing doctrine that finds standing based on a statutory violation regardless of whether a harm has occurred does not conflict with an analysis that considers a future harm an injury in fact. Instead, it should be seen as an alternative for when the alleged injuries are based on a statutory right.[299] This does not require that an injury in fact be "actual or imminent" and "concrete or particularized" because if a statutory right has been violated, an injury in fact is present.[300] The Supreme Court has reasoned that the violation of a statute creates an injury, a disregard for legislatively created legal rights, that establishes standing, whether or not the violation resulted in a monetary harm.[301] While the Supreme Court has ruled that not all statutory violations automatically create standing, unauthorized disclosures of information have been interpreted to satisfy the injury in fact requirement.[302] Therefore, the Third Circuit's ruling in *Horizon Healthcare* is not contradictory to an analysis that considers the risk of future harm an injury in fact

---

[296] *Id.* at 560–61.

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

[298] *Lujan*, 504 U.S. at 578 ("[T]he . . . injury required by Art. III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" (citations omitted)).

[299] *See id.*

[300] *Id.* at 560, 578.

[301] *Id.* at 578.

[302] *See, e.g.*, Spokeo, Inc v. Robins, 136 S. Ct. 1540, 1549 (2016); *In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 273 (3d Cir. 2017).

but is instead a separate and reliable analysis for when statutory rights are violated.[303]

CONCLUSION

Interpreting standing doctrine to consider the risk of future harm sufficient to establish standing would create a uniform application of standing. Additionally, it would enable victims of data breaches to obtain justice and encourage entities that hold personal information to improve their security measures.[304] This uniform application of standing doctrine is clearly necessary because of the circuit split with regard to conferring standing between the Second[305] and Fourth Circuits[306] and the D.C.,[307] Sixth,[308] Seventh,[309] Eighth,[310] and Ninth Circuits.[311] Additionally, as the number of data breaches continues to increase, an interpretation of standing doctrine where (1) the risk of a future harm creates standing and (2) a statutory violation creates standing regardless of whether harm actually occurred will allow plaintiffs to achieve a remedy for the failure of others to safeguard their information.[312] This increase

---

[303] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 634–35 (3d Cir. 2017).

[304] *See* Bill Sampson, Al Saikali, & Dan Schwaller, *A Changing Legal Landscape and a Few Suggestions for Counsel*, SHOOK, HARDY & BEACON L.L.P., https://www.shb.com/intelligence/publications/2016/q1/sampson-saikali-and-schwaller-pen-piece (last visited Sept. 18, 2019). *See generally* LEBLANC & KNIGHT, *supra* note 62 (discussing how improvements in standing requirements may encourage "pre-breach [company] compliance" and provide plaintiffs with additional grounds to bring suit).

[305] Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017).

[306] Beck v. McDonald, 848 F.3d 262, 274–78 (4th Cir. 2017).

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

[308] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–91 (6th Cir. 2016).

[309] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015).

[310] *In re* SuperValu, Inc., 870 F.3d 773, 772–74 (8th Cir. 2017).

[311] Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010).

[312] *Data Breaches Compromised 4.5 Billion Records in First Half of 2018*, *supra* note 39. *See generally* LEBLANC & KNIGHT, *supra* note 62 (discussing how

in legal action should push entities to spend more money on data protection because the increasing rate of data breach litigation indicates such entities have not found the motivation elsewhere.[313]

using future risk of harm and statutory violations to create standing will provide plaintiffs with a valuable remedy).

[313] LEBLANC & KNIGHT, *supra* note 62, at 4 (noting that "pre-breach compliance" may prepare counsel for "increasingly inevitable post-breach litigation").