Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution

PATRICK J. LORIO*

As businesses and individuals increasingly rely on electronic technology to facilitate transactions, hackers have taken advantage of the weaknesses of data security systems intended to protect sensitive information. As a result, hackers have gained access to individuals' personal and financial information. American law, however, has been slow to catch up to the threat posed by data security breaches. Although breaches have become commonplace in the past decade, victims of data breaches are often denied their day in court. Instead, many federal courts find that plaintiffs who sue companies for failing to adequately protect their private information lack Article III standing, the constitutional doctrine that requires plaintiffs to show an "injury-in-fact" in order to sue in federal court. While some jurisdictions hold that hackers having access to individuals' information is sufficient to confer Article III standing, other jurisdictions dismiss plaintiffs' cases unless the plaintiffs can demonstrate unreimbursed financial loss directly attributable to the data breach, a very high bar to reach.

The purpose of this Note is threefold. First, I analyze the existing split within the U.S. Courts of Appeals with regard to the correct theory of Article III standing to apply in data breach cases. The circuit split primarily involves disputes over the correct interpretation of Clapper v. Amnesty International*, a 2013 U.S. Supreme Court case dealing with the "imminency" requirement of Article III standing's injury-in-fact component. Second, I predict what the recent holding in* Spokeo v. Robbins *(2016) portends for data breach victims.* Spokeo *heightened the scrutiny that federal courts must place on the "concreteness" of injury in addition to the inquiry into "imminency." Finally, I propose that the strict*

---

* Notes Editor, Colum. J.L. & Soc. Probs., 2017–2018. J.D. Candidate 2018, Columbia Law School. The author extends his thanks to the staff members of the *Columbia Journal of Law and Social Problems* and his advisor, Professor Philip Genty, for their helpful feedback. The author also thanks Garrett Cain and his family for their constant support.

Article III standing requirements articulated by the Supreme Court in both Clapper *and* Spokeo *necessitate action by Congress. I argue that Congress should pass a comprehensive data breach statute that would confer standing upon victims of data breach. I conclude by showing how a recent Third Circuit decision demonstrates the viability of a statutory solution to the problem encountered by data breach victims.*

I. DATA BREACHES: AN OVERVIEW

On September 22, 2016, technology company Yahoo! announced that a third party had wrongfully gained access to at least 500 million Yahoo! user accounts, the largest data breach[1] in history.[2] Hackers stole individuals' names, telephone numbers, email addresses, dates of birth, passwords, and security questions and answers.[3] Because individuals often use the same email address, password, and security questions for multiple Internet accounts, the third party hacker could potentially gain access to additional private accounts, including financial accounts, of 500 million individuals.[4]

More recently, Equifax — a major credit-reporting firm — announced that hackers accessed the personal information of more than 140 million U.S. customers.[5] The obtained information includes individuals' names, addresses, Social Security numbers, and driver's license numbers.[6] The hackers could use this extensive information to open new financial accounts in individuals' names, make fraudulent charges on their credit cards, and commit tax fraud.[7] Due to the scope of the breach, the affected individuals will have to monitor their credit and personal accounts for the rest of their lives because hackers can use the stolen in-

1. Broadly defined, a "data breach" occurs when "a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information." In the Matter of Protecting the Privacy of Customers of Broadband & Other Telecommunications Servs., 31 FCC Rcd. 2500 (2016). As used in this Note, a "hacker" is the person or entity who, without authorization, accesses the information.

2. Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), http://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=0 [https://perma.cc/G5RK-YSTE].

3. *Id.*

4. *Id.*

5. Paresh Dave, *Credit giant Equifax says Social Security numbers, birth dates of 143 million consumers may have been exposed*, L.A. TIMES (Sept. 7, 2017), http://www.latimes.com/business/technology/la-fi-tn-equifax-data-breach-20170907-story,amp.html [https://perma.cc/CVU3-36R6].

6. *Id.*

7. *Id.*

formation for many years going forward to commit fraud, including "creating a new you."[8]

The data breaches of Yahoo! and Equifax are two of the largest known data breaches and are part of a trend in recent years in which the size and scope of data breaches of major corporations have steadily increased.[9] This trend is expected to continue as hackers become increasingly sophisticated and more personal information is stored digitally.[10] Federal courts' interpretations of Article III standing requirements, however, frequently result in unjust outcomes for data breach victims.[11] In everyday life, individuals provide businesses and other entities with their personal information. Indeed, it is inconceivable that individuals could successfully function in the modern world without sharing such information. Yet when the information falls into the hands of hackers, individuals may suffer identity theft, fraudulent credit card charges, and other consequences. Individuals whose private information is accessed therefore reasonably expend considerable time, energy, and money protecting their identity and financial accounts by purchasing credit-monitoring services, monitoring their accounts for fraudulent charges, disputing any fraud that occurs, and paying fees associated with credit freezes.

In order to recover the costs incurred following a data breach, data breach victims frequently attempt to sue the companies that failed to adequately protect their information from hackers.[12] Some federal courts, however, have found that data breach victims cannot satisfy Article III standing requirements. As a result, courts dismiss lawsuits against the organizations that allowed victims' information to be accessed due to insufficient data security safeguards. While this outcome may be justified legally

---

8. Adam Shell, *Equifax data breach could create lifelong identity theft threat*, USA TODAY (Sept. 9, 2017), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/ [https://perma.cc/GTZ5-HA6X].

9. Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 12, 2016), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/9RRB-P8VV]; *see also* Heather Landi, *Report: Healthcare Data Breaches Continue at Alarming Pace in Second Half of 2016*, HEALTHCARE INFORMATICS (Oct. 17, 2016), http://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-data-breaches-continue-alarming-pace-second-half-2016 [https://perma.cc/9XUP-VBGF].

10. Lord, *supra* note 9; *see also* Landi, *supra* note 9.

11. I use the term "data breach victims" to refer to those individuals whose private information was allegedly exposed — rather than merely accessed — in a data breach.

12. In most cases, the hacker is unknown, so individuals cannot directly sue the hacker.

under current Article III jurisprudence, many victims of data breaches cannot recover the costs they incur in response to a data breach.

This Note attempts to propose a solution to the immediate dilemma faced by many victims of data breaches — that they cannot even get their day in court. First, I briefly review the constitutional law doctrine of Article III standing, focusing primarily on the injury-in-fact requirement.[13] I then turn to a survey of the different approaches to Article III standing in data breach cases as applied in various federal jurisdictions and look at the impact of the recent U.S. Supreme Court decision in *Spokeo v. Robbins* on data breach litigation going forward.[14] I conclude with a proposed solution to the Article III hurdles faced by data breach plaintiffs by arguing that Congress should pass a comprehensive law regulating data breaches that would afford victims statutory standing to pursue their claims against companies that fail to adequately protect their information.[15]

II. AN INTRODUCTION TO ARTICLE III STANDING

In order to litigate in federal courts,[16] plaintiffs must satisfy the U.S. Constitution's Article III standing requirements. Article

13. *Infra* Part II.

14. *Infra* Parts III and IV.

15. *Infra* Part V.

16. Data breach cases are generally litigated in federal court. Under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1453 (2005), diversity jurisdiction can be invoked in a class action lawsuit if there is minimal — rather than complete — diversity. In the non-class action context, diversity jurisdiction exists only if none of the plaintiffs reside in the same state as any defendant (complete diversity) and the amount in controversy exceeds $75,000. 28 U.S.C. § 1332 (as amended 2005). In class actions, diversity jurisdiction is appropriate if at least one plaintiff resides in a different state than at least one defendant (minimal diversity) and the aggregate sum of each individual plaintiff's claims is at least $5 million. 28 U.S.C. § 1332(d)(2). CAFA has generally been viewed as a tool for limiting class actions because federal courts must apply the strict requirements of Fed. R. Civ. P. 23 as well as consider issues such as Article III standing. In contrast, many states place more lax rules on class actions. Consequently, defendants can more easily defeat class actions on procedural grounds in federal court and will remove class actions to federal courts under diversity jurisdiction if originally filed in state courts. *See, e.g.*, Jean Macchiaroli Eggen, *The Impact of the Class Action Fairness Act on Plaintiffs in Mass-Tort Actions*, 12 ANDREWS CLASS ACTION LITIG. REP. 17 (2005); Thomas E. Willging & Shannon R. Wheatman, Fed. Judicial Ctr., *An Empirical Examination of Attorneys' Choice of Forum in Class Action Litigation* (2005), *available at* http://www.uscourts.gov/sites/default/files/clact05.pdf [https://perma.cc/VYU4-FWU5].

III standing is an aspect of justiciability,[17] the principle that ensures federal courts only resolve "cases" or "controversies," or actual, ongoing disputes, between the parties.[18] "Cases" and "controversies" stand in contrast to advisory opinions — decisions advising a course of action before a dispute actually arises — or decisions affecting a litigant no differently than the public at large. The primary justification for the Article III standing doctrine is the concept of separation of powers.[19] Article III, by limiting the disputes courts are called to resolve, helps to ensure that federal courts do not "usurp the powers of the political branches."[20] Instead of broadly "making law" absent a specific controversy between particular litigants, Article III standing requirements purport to allow federal courts to only resolve those disputes arising under *existing* law.[21]

As articulated by the U.S. Supreme Court in *Lujan v. Defenders of Wildlife*, Article III standing depends on three primary factors:

> First, the plaintiff must have suffered an "injury-in-fact" — an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical[.] Second, there must be a caus-

17. For an overview of the doctrines of justiciability, *see* Jonathan R. Siegel, *A Theory of Justiciability*, 86 TEX. L. REV. 73 (2007).

18. Warth v. Seldin, 422 U.S. 490, 498 (1975); *see also* U.S. CONST. art. III, § 2 ("The judicial power shall extend to all cases, in law and equity, arising under this Constitution, the laws of the United States, and treaties made, or which shall be made, under their authority;--to all cases affecting ambassadors, other public ministers and consuls;--to all cases of admiralty and maritime jurisdiction;--to controversies to which the United States shall be a party;--to controversies between two or more states;--between a state and citizens of another state;--between citizens of different states;--between citizens of the same state claiming lands under grants of different states, and between a state, or the citizens thereof, and foreign states, citizens or subjects.").

19. For an overview of Article III standing as it relates to the theory of separation of powers, *see* F. Andrew Hessick, *The Separation-of-Powers Theory of Standing*, 95 N.C. L. REV. 673, 685 (2017), Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U.L. REV. 881, 881 (1983) ("[J]udicial doctrine of standing is a crucial and inseparable element" of the separation of powers.), and Maxwell L. Stearns, *Spokeo, Inc. v. Robins and the Constitutional Foundations of Statutory Standing*, 68 VAND. L. REV. EN BANC 221 (2015).

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

21. *See* John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1229–31 (1993) ("Separation of powers is a zero-sum game. If one branch unconstitutionally aggrandizes itself, it is at the expense of one of the other branches. . . . [Standing] does derive from and promote a conception that judicial power is properly limited in a democratic society. That leaves greater responsibility to the political branches of government — however they are inclined.").

> al connection between the injury and the conduct complained of — the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be "likely," as opposed to merely "speculative," that the injury will be redressed by a favorable decision.[22]

In order for a court to reach the second and third prongs of the Article III analysis — causality and redressability, respectively — the plaintiff must first show an "injury-in-fact." In fact, the Supreme Court has found that injury-in-fact is the "[f]irst and foremost of standing's three elements."[23] As *Lujan* indicates, demonstrating "injury-in-fact" turns on the plaintiff's ability to show the violation of a legal right that is "actual or imminent" as well as "concrete and particularized."[24] Because the question of Article III standing in data breach cases turns primarily on the "injury-in-fact" analysis,[25] I shall spend the majority of this Note analyzing the elements of "injury-in-fact" in connection with data breach litigation.

A. "ACTUAL OR IMMINENT"

To date, federal judges have primarily focused their Article III standing inquiry in data breach cases on the "actual or imminent" requirement of injury-in-fact.[26] Therefore, I begin with an overview of what I will call the "imminency" requirement of Article III.

The U.S. Supreme Court gave its most recent and detailed articulation of the imminency requirement in *Clapper v. Amnesty*

---

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

23. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Steel Co. v. Citizens for Better Environment, 523 U.S. 83, 103 (1998)).

24. *Lujan*, 504 U.S. at 560–61.

25. For a discussion on the difficulty of proving causation in data breach cases, *see* John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 961 (2016); Elizabeth T. Isaacs, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 546–548 (2015).

26. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

International.[27] In *Clapper*, human rights, legal, and media organizations argued that Section 702 of the Foreign Intelligence Surveillance Act (FISA) was unconstitutional. Section 702 allows the U.S. government to conduct surveillance of non-U.S. citizens believed to be located outside of the United States in order to gather intelligence. The government must first seek approval from the Foreign Intelligence Surveillance Court (the "FISA Court").[28]

The *Clapper* plaintiffs asserted that they communicated with individuals outside of the United States who were likely to be targeted for surveillance under FISA. They argued that Section 702 "compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[29] The plaintiffs further contended that FISA caused them to "have ceased engaging" in certain telephone and e-mail conversations, and therefore they would have to travel outside of the U.S. in order to have confidential communications with their sources and clients.[30]

Without reaching the merits of their argument, the Court held that the *Clapper* plaintiffs lacked Article III standing because their injury was not "actual or imminent."[31] While the plaintiffs claimed that they suffered an injury because there was "an objectively reasonable likelihood that their communications with their foreign contacts will be intercepted . . . at some point in the future," the Court disagreed.[32] Instead, as Justice Alito wrote for the Court, the plaintiffs' theory of standing relied on "a highly attenuated chain of possibilities"[33] because the plaintiffs had no knowledge that the government had actually intercepted or targeted communications to which they were a party.[34] Moreover, the Court held that plaintiffs could not establish standing simply

27. Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
28. 50 U.S.C. § 1881a (2015).
29. *Clapper*, 568 U.S. at 406.
30. *Id.*
31. *Id.* at 422.
32. *Id.* at 410.
33. In order for an injury to occur: (1) the government would have to decide to target those individuals with whom the plaintiffs communicate; (2) the government would have to invoke Section 702 of FISA, rather than some other statutory provision that authorizes surveillance, (3) the FISA Court would have to approve the government's request, (4) the government would have to actually succeed in intercepting communications from the target, and (5) the communications intercepted would have to be those to which plaintiffs were a party. *Id.*
34. *Id.* at 410–11.

by paying for travel in order to hold in-person conversations rather than communicate via telephone or e-mail. To decide otherwise, the Court said, would allow "an enterprising plaintiff . . . to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."[35] The *Clapper* Court concluded by holding that an allegation of future injury will satisfy the imminency requirement of Article III only if the threatened injury is "certainly impending," or there is a "'substantial risk' that the harm will occur."[36] This requirement meant that the *Clapper* plaintiffs would have had to show that they incurred costs in the face of a "threat of certainly impending interception" in order to satisfy the imminency requirement.[37]

Following *Clapper*, it is clear that Article III standing exists only if federal courts can identify an injury that has already occurred or a non-speculative and highly probable risk of injury in the near future. In the context of data breach litigation, this requirement raises a dilemma for plaintiffs. In many cases, the plaintiffs' injury — fraudulent charges — has not yet occurred and may never occur. Questions arise, for example, as to whether hackers understand the data they obtain.[38] Nonetheless, plaintiffs reasonably spend time and money on credit monitoring and other fraud-prevention services. Showing imminency of injury, therefore, is the first — and perhaps biggest — obstacle for individuals seeking to recover the resources they expend in response to a data breach.

B. "CONCRETE AND PARTICULARIZED"

While the Supreme Court's articulation of the elements of Article III standing in *Lujan* seemingly treats "concrete and particularized" as one element of the "injury-in-fact" prong of analysis, the Court has subsequently noted that concreteness and particularization are two distinct and meaningfully different elements that plaintiffs must satisfy.[39] As such, it is important to analyze each in turn.

---

35. *Id.* at 416.
36. *Id.* at 414 n.5.
37. *Id.* at 417.
38. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).
39. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) ("Particularization is necessary to establish injury-in-fact, but it is not sufficient . . . . [A]n injury-in-fact must be both concrete and particularized.").

1. *Particularized*

An injury is considered "particularized" when it affects the plaintiff "in a personal and individual way."[40] A plaintiff cannot simply allege a public harm or the violation of a "public right," such as the breach of a duty owed to the community as a whole.[41] For example, a plaintiff alleges a sufficiently particularized injury if she claims that the defendant's violation of a statute or common law duty led directly to her harm, rather than harm to other parties not before the court or harm to the general public.[42] By contrast, private citizens cannot sue to "vindicate the constitutional validity of a generally applicable law" when they do not "possess a 'direct stake in the outcome' of the case."[43] In such circumstances, plaintiffs would be unable to allege a particularized injury because they would have "no 'personal stake' in defending its enforcement that is distinguishable from the general interest of every [other] citizen."[44]

2. *Concrete*

In contrast to a "particularized" injury, a "concrete" injury is somewhat more difficult to identify or define. Prior to the *Spokeo* decision in 2016, the Supreme Court focused little of its Article III standing jurisprudence on concreteness of injury. Nonetheless, *Spokeo* brought to light new concerns for plaintiffs seeking to establish standing in federal courts.[45]

The *Spokeo* plaintiff brought a class action lawsuit against the website Spokeo, a "people search engine,"[46] for alleged violations

40. Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 n.1 (1992).

41. *See Spokeo*, 136 S. Ct. at 1551–1552 (Thomas, J. concurring).

42. *Id*. at 1548 (majority opinion) (quoting Robins v. Spokeo, 742 F.3d 409, 413 (9th Cir. 2014)) ("Robins's personal interests in the handling of his credit information are *individualized rather than collective*.").

43. Hollingsworth v. Perry, 133 S. Ct. 2652, 2662 (2013) (holding that petitioners, ordinary California citizens, did not satisfy Article III standing when appealing a federal district court decision that held Proposition 8, a state constitutional amendment banning same-sex marriage, unconstitutional because the outcome of the case did not personally affect the petitioners).

44. *Id.* at 2663.

45. *See Spokeo*, 136 S. Ct. at 1540.

46. The Court assumed that defendant Spokeo qualified as a "consumer reporting agency" subject to the rules under the Federal Credit Reporting Act. *Spokeo*, 136 S. Ct. at 1546 n.4.

of the Fair Credit Reporting Act (FCRA).[47] The plaintiff sought damages from the website and claimed that *Spokeo* violated the FCRA by gathering and disseminating false information about individuals, including himself. The FCRA provides that "[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any [individual] is liable to that [individual]" for either "actual damages" or statutory damages of $100 to $1,000 per violation.[48]

The *Spokeo* plaintiff alleged that an unknown third party searched his name on Spokeo's website and the search returned inaccurate information on his age, marital status, education, and finances.[49] The complaint further alleged that Spokeo willfully violated the FCRA's requirements that consumer reporting agencies "follow reasonable procedures to assure maximum possible accuracy" of consumer reports.[50] The U.S. District Court for the Central District of California found that the plaintiff failed to show an injury-in-fact, but the Ninth Circuit reversed, noting that "[the plaintiff's] personal interests in the handling of his credit information are individualized rather than collective" — thus satisfying the "particularized" requirement. The Ninth Circuit then explicitly addressed concreteness, albeit in a conclusory manner, simply stating that "the interests protected by the statutory rights at issue are sufficiently concrete and particularized that Congress can elevate them."[51] The U.S. Supreme Court reversed and remanded the Ninth Circuit's decision, finding that the appellate court failed to engage in meaningful analysis of the concreteness requirement of injury-in-fact.

In detailing what is required for an injury to be "concrete," the Court said that a "'concrete' injury must be 'de facto'; that is, it must actually exist."[52] The injury must be "real" as opposed to "abstract."[53] The Court also cautioned that "concrete" does not necessarily mean "tangible."[54] While tangible injuries — such as loss of money — are perhaps the easiest to recognize as concrete,

47. *Id.* at 1544.
48. 15 U.S.C. § 1681n(a) (2008); *Spokeo*, 136 S. Ct. at 1545.
49. *Spokeo*, 136 S. Ct. at 1546.
50. 15 U.S.C. § 1681e(b) (2008); *Spokeo*, 136 S. Ct. at 1546.
51. Robins v. Spokeo, Inc., 742 F.3d 409, 413 (9th Cir. 2014) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)).
52. *Spokeo*, 136 S. Ct. at 1548 (citing Black's Law Dictionary 479 (9th ed. 2009)).
53. *Id.*
54. *Id.* at 1549.

intangible harm may also be concrete depending on "both history and the judgment of Congress."[55] The Court also reiterated its prior holding that Congress can "elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law."[56]

However, despite Congress' power to elevate intangible harm to the level of necessary concreteness for Article III standing, the Court also cautioned that a plaintiff does *not* "automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[57] A mere procedural violation of a statute, for example, does not result in a concrete injury.[58] Applying this rule to the plaintiff's claim against Spokeo, the Court wrote:

> A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.[59]

The Court therefore signaled that the potential or actual *consequences* of an alleged injury are also an important factor in the Article III standing inquiry.

In the *Spokeo* decision, the Court also connected the imminency requirement with concreteness, stating that the *risk* of real harm can sometimes satisfy concreteness.[60] The Court qualified that such a circumstance would arise when a plaintiff could al-

---

55. *Id.*
56. *Id.* (citing *Lujan*, 504 U.S. at 578).
57. *Id.*; *see also infra* Part V.B.
58. *Spokeo*, 136 S. Ct. at 1550.
59. *Id.* at 1550.
60. *Id.* at 1549 ("This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness. . . . [T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury-in-fact.") (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)).

lege the particular harm that Congress intended to remedy when passing a specific statute.[61] To support this proposition — which seemingly contradicts the Court's allegation that a plaintiff must allege some injury beyond a mere procedural violation of a statute — the Court cited two cases in which particular federal agencies refused to release information that Congress mandated the agencies disclose to the public.[62] The contradiction can be resolved, however, by viewing the particular injuries suffered by the plaintiffs in the mandated-disclosure cases as exactly the type of injuries the relevant laws were intended by Congress to prevent.[63]

The FCRA requires credit-reporting agencies to act reasonably in ensuring accuracy and permits individuals to sue agencies for violations, but the law does not explicitly give individuals the right to be free from all inaccurate information. As previously noted, Congress presumably did not consider the inaccurate reporting of a zip code to be a harm deserving a remedy when drafting and passing the FCRA.[64] Because it was unclear whether Congress intended to remedy an injury resulting from the type of misinformation disseminated by Spokeo about the plaintiff, the Court could not conclude that the plaintiff's intangible injury was sufficiently "concrete." Had plaintiff alleged a tangible injury, such as loss of income or job opportunity due to the misinformation, the concreteness requirement likely would have been satisfied.[65]

---

61. *Id.* at 1549–1550.

62. *Id.* (citing Federal Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998); Public Citizen v. Dep't of Justice, 491 U.S. 440, 449 (1989)).

63. Contrast *Akins* and *Public Citizen* with United States v. Richardson, 418 U.S. 166 (1974). In *Richardson*, the plaintiff sought information from the CIA under the U.S. Constitution's Accounts Clause. Art. I, § 9, cl. 7. The U.S. Supreme Court found that the plaintiff failed to satisfy Article III standing because he did not allege an "injury-in-fact." Richardson, 418 U.S. at 179–180. But, had Congress provided citizens with a right to such information — and had the plaintiff suffered the type of injury Congress intended the statute to rectify — the plaintiff would likely have satisfied Article III standing. *See Akins*, 524 U.S. at 21–22.

64. The Court recognized that the *Spokeo* plaintiff alleged injuries other than the inaccurate reporting of a zip code, including inaccurate information on his education level and wealth, but remanded the case to the Ninth Circuit to determine whether such injuries were "concrete." *Spokeo*, 136 S. Ct. at 1550 n.8.

65. On remand, the Ninth Circuit concluded that the *Spokeo* plaintiff alleged a sufficiently concrete injury. Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017) ("[W]e conclude that the FCRA procedures at issue in this case were crafted to protect consumers' (like Robins's) concrete interest in accurate credit reporting about themselves."). Given the skepticism expressed by the Supreme Court of liberal theories of Article III standing,

III. THE CURRENT LAW: STANDING IN DATA BREACH CASES

The application of Article III standing in data breach cases is currently in flux. The Supreme Court has never decided the issue of Article III standing in the context of data breaches, and data breaches present unique problems for the Article III injury-in-fact analysis. The Sixth, Seventh, Ninth, and D.C. Circuits appear to strongly favor standing in data breach cases. In contrast, the Third,[66] Fourth, and Eighth Circuits, as well as some federal district courts, appear to disfavor standing unless the plaintiff can show financial loss sufficiently traceable to the breach. Importantly, however, many of these jurisdictions have yet to address standing in data breach cases in light of the recent *Spokeo* decision; as such, many decisions do not engage in a meaningful "concreteness" inquiry, instead focusing on the imminency requirement.[67] Even those courts that have issued decisions following *Spokeo* do not adequately address concreteness in a manner likely to satisfy the Supreme Court. In this part, I outline the current state of law in each of the aforementioned jurisdictions.

A. LIBERAL THEORIES OF STANDING IN DATA BREACH CASES

The Sixth, Seventh, Ninth, and District of Columbia Circuit Courts of Appeals have adopted the most liberal theories of Article III standing, allowing data breach victims to sue whenever their personal information is exposed to hackers. For example, many data breach cases in these circuits involve a data breach where the plaintiffs have not yet received fraudulent credit charges[68] and/or it is unclear whether the hackers even understood the data.[69] Injury, instead, is claimed to result from the financial loss suffered because plaintiffs must pay for credit monitoring and other fraud-prevention services.

---

however, it is unclear how much weight should be given to the Ninth Circuit's concreteness analysis in the remand decision.

66. *But see infra* Part V.D.

67. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

68. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).

69. *See, e.g.*, *In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2012).

1. *The Seventh Circuit*

The most influential opinion from the Seventh Circuit on this question is *Remijas v. Neiman Marcus*.[70] In *Remijas*, approximately 350,000 credit cards were exposed to hackers, and 9,000 of those cards were then used fraudulently.[71] When the department store chain Neiman Marcus disclosed the data breach, plaintiffs filed a class action lawsuit alleging negligence, breach of implied contract, and unjust enrichment, among other state law claims.[72] Notably, none of the plaintiffs who had suffered fraudulent charges could show that the charges were the result of the Neiman Marcus data breach, and several other major data breaches of credit card information were known to have occurred around the same time as the Neiman Marcus breach.[73] Additionally, "the *overwhelming majority* of the plaintiffs allege[d] only that their data may have been stolen" and could not point to any fraudulent activity whatsoever.[74]

Citing *Clapper*, the Seventh Circuit nonetheless found that the *Remijas* plaintiffs satisfied Article III standing. The Seventh Circuit emphasized that some plaintiffs had actually suffered fraudulent credit card charges. The court explained that "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[75] The court noted that the very purpose of a data breach is to obtain — and use — consumers' information, and hackers may continue to use the information for many years;[76] in the meantime, plaintiffs continue to spend time and money on credit monitoring and similar services.[77]

The *Remijas* decision distinguished *Clapper*, framing *Clapper* as a case about "speculative harm based on something that may

70. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).
71. *Id.* at 690.
72. Remijas v. Neiman Marcus Grp., LLC, No. 14-C-1735, 2014 WL 4627893, at *1 (N.D. Ill. Sept. 16, 2014).
73. *Remijas*, 794 F.3d at 690.
74. *Remijas*, 2014 WL 4627893, at *3 (emphasis added).
75. *Remijas*, 794 F.3d at 693 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).
76. The Seventh Circuit appears to not have considered the fact that plaintiffs could cancel credit cards at any time.
77. *Remijas*, 794 F.3d at 693–694.

not even have happened to some or all of the plaintiffs."[78] In contrast, the Seventh Circuit concluded, Neiman Marcus admitted that the "something," the data breach, had already occurred and that plaintiffs' information was exposed.[79] As such, there was a "substantial risk" of injury due to the data breach, satisfying the *Clapper* standard.[80]

More recently, the Seventh Circuit revisited the question of Article III standing in the data breach context in *Lewert v. P.F. Chang's*[81] and adopted an even more liberal theory of standing. The facts of *Lewert* are similar to *Remijas*. P.F. Chang's, a national restaurant chain, announced that one of its locations in Illinois had suffered a data breach. Both of the named plaintiffs paid with debit cards. One of the named plaintiffs, Kosner, suffered four fraudulent charges, but subsequently cancelled the debit card.[82] The other plaintiff, Lewert, did not suffer any fraudulent charges and did not cancel his debit card. Nonetheless, both plaintiffs asserted that they were injured because they spent time and money monitoring their credit.[83] The named plaintiffs had not dined at the location named by P.F. Chang's as affected by the breach, but rather dined at a different P.F. Chang's location.[84]

The Seventh Circuit held that the *Lewert* plaintiffs suffered a "substantial risk of harm" that their debit card information *would be used* to incur fraudulent charges.[85] Because of the substantial risk of harm — satisfying *Clapper*'s imminency requirement — the time, effort, and money spent resolving and monitoring potential fraudulent activity were sufficiently "concrete" injuries.[86] Notably, the court held that it was immaterial that Kosner and similarly situated plaintiffs were fully reimbursed for fraudulent charges and therefore suffered no out-of-pocket financial loss because of the effort expended as a result of the fraud.[87] The court also rejected P.F. Chang's argument that plaintiffs did not dine at the location affected by the data breach and thus had not

78. *Id.* at 694.
79. *Id.*
80. *Id.* at 693.
81. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).
82. *Id.* at 965.
83. *Id.*
84. *Id.* at 965.
85. *Id.* at 967.
86. *Id.*
87. *Id.*

suffered injury, finding that the extent of the data breach was a question to be solved by the fact-finder at trial rather than at the motion to dismiss stage, where courts must accept a plaintiff's allegations as true.[88] Due to these facts, *Lewert* stands today as arguably the most expansive approach to Article III standing in the data breach context.

2. *The Ninth Circuit*

The Ninth Circuit has found Article III standing requirements satisfied "where a plaintiff alleges that his personal information was collected and then wrongfully disclosed."[89] The landmark Ninth Circuit precedent came in *Krottner v. Starbucks*.[90] The *Krottner* plaintiffs were a group of Starbucks employees. In 2008, an unknown individual stole a company laptop containing the names, addresses, and social security numbers of 97,000 Starbucks employees.[91] Starbucks notified the affected employees about the breach and offered the individuals free credit monitoring services.[92] Although none of the plaintiffs suffered any financial loss, they alleged an injury due to the time spent monitoring their accounts.[93] The court found that the plaintiffs suffered "a credible threat of harm" that was "real and immediate."[94] Consequently, the court held "that [individuals] whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III.[95]

Although the Ninth Circuit has not revisited Article III standing in data breach cases post-*Clapper*, district courts within the circuit have relied on the *Krottner* analysis in upholding standing for data breach plaintiffs. A judge in the U.S. District Court for the Southern District of California found that under *Clapper* and *Krottner*, plaintiffs are also *not* required to allege that their personal information was "actually accessed by a third party."[96] Instead, the district court found, it sufficed that hackers breached

88. *Id.* at 967–968.
89. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961–62 (S.D. Cal. 2014).
90. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
91. *Id.* at 1140.
92. *Id.* at 1140–1141.
93. *Id.* at 1141.
94. *Id.* at 1143.
95. *Id.* at 1140.
96. *In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014).

the defendant's system and *could* have accessed such information.[97]

3. *The Sixth Circuit*

In late 2016, following the Supreme Court's *Spokeo* decision, the Sixth Circuit released its decision in *Galaria v. Nationwide Mutual Insurance*.[98] Defendant Nationwide is an insurance and financial services company that maintains customers' birth dates, marital statuses, employers, Social Security numbers, and driver's license numbers.[99] In 2012, hackers accessed this data.[100] In response, Nationwide offered one year of free credit monitoring and identity-fraud protection to the one million individuals whose information had been accessed.[101]

Like the Seventh and Ninth Circuits, the Sixth Circuit focused its Article III inquiry on imminency. The Sixth Circuit decided that because the data breach targeted personal information, "a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes" even though there had been no fraudulent activity yet.[102] Because there was a "sufficiently substantial risk of harm" resulting from fraud, incurring mitigation expenses was reasonable. Because Nationwide only provided credit monitoring for one year and did not reimburse victims for credit freezes, the court held that the plaintiffs satisfied the injury-in-fact requirement.[103]

Although *Galaria* is one of the few data breach cases decided after *Spokeo*, the Sixth Circuit did not thoroughly address concreteness and did not even cite to *Spokeo* when discussing concreteness. Rather, the court simply found that the plaintiffs'

---

97. *Id.*; *see also In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014) (finding that plaintiffs had standing when hackers accessed plaintiffs' credit card information despite no allegations that the plaintiffs' credit cards had been misused). *But see In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (finding that plaintiffs' claim fails the imminency requirement of Article III standing because there was no evidence that plaintiffs' information was used in three years since the initial data breach; the passage of time evidences that a "substantial risk" that harm will occur does not exist).

98. Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x. 384 (6th Cir. 2016).

99. *Id.* at 386.

100. *Id.*

101. *Id.*

102. *Id.* at 388.

103. *Id.*

"costs are a concrete injury."[104] Consequently, *Galaria* offers little predictive value as to how other courts — and ultimately the Supreme Court — will treat concreteness in the data breach context. Nonetheless, this cursory concreteness analysis will be unlikely to persuade other courts attempting to follow *Spokeo*. The Sixth Circuit simply assumed that because the plaintiffs' information was "stolen" by hackers, there was a "substantial risk" of harm — in the form of future fraudulent activity related to the stolen data — necessary to find injury.[105] Yet, in *Spokeo*, the Supreme Court found that the risk of future harm only satisfies concreteness under certain circumstances.[106] Specifically, the Court mentioned instances where common law has "long permitted recovery . . . even if their harms may be difficult to prove or measure" and limited instances in which a statute specifically identifies a harm.[107] It is unclear on what basis the Sixth Circuit found that the risk of future fraudulent activity could be considered a concrete injury, especially if there is no indication that the hackers can or will use the data to the detriment of plaintiffs.

4. *The D.C. Circuit*

In *Attias v. Carefirst, Inc.*, an insurance provider, CareFirst, suffered a data breach.[108] Although it remains undetermined whether hackers accessed individuals' social security number, or merely their addresses and customer identification numbers — and no individual suffered fraudulent activity or identify theft — plaintiffs sued CareFirst for breach of contract and negligence.[109] The U.S. District Court for the District of Columbia held that the plaintiffs lacked Article III standing because any alleged harm was too speculative due to the fact that "[p]laintiffs have not suggested, let alone demonstrated, how the CareFirst hackers could steal their identities without access to their social security or credit card numbers."[110]

---

104. *Id.* at 389.
105. *Id.* at 388.
106. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).
107. *Id.* (citing Federal Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998); Restatement (First) of Torts § 569 (libel)).
108. Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).
109. *Id.* at 623.
110. Attias v. CareFirst, Inc., 199 F. Supp. 3d 193, 201 (D.D.C. 2016).

On appeal, the D.C. Circuit reversed the district court and held that the plaintiffs satisfied Article III standing. Although *Attias* was decided after *Spokeo*, the D.C. Circuit did not analyze the concreteness of the plaintiffs' claims, stating only that "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."[111] The court did not address the fact that none of the plaintiffs actually alleged identify theft or that it was unclear if the hackers even stole the type of information that would be required for identify theft to be committed in the future. Instead, the D.C. Circuit focused its analysis on the imminency requirement. Citing to the Seventh Circuit's *Remijas* decision, the court explained that "an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative — at the very least, it is plausible — to infer that this party has both the intent and the ability to use that data for ill."[112]

B. RESTRICTIVE THEORIES OF STANDING

In contrast to the more liberal Article III standing approaches in data breach cases adopted by the Sixth, Seventh, Ninth, and D.C. Circuits, the Third, Fourth, and Eighth Circuits, as well as district courts within other circuits, require a higher threshold for plaintiffs seeking to establish injury-in-fact. Plaintiffs cannot merely allege that hackers potentially accessed private information. Instead, these courts require evidence that the data was actually used to the detriment of the victims or, at the very least, that the hackers could understand the accessed data and have actual plans to misuse it.

1. *The Third Circuit*

The Third Circuit approach to Article III standing in data breach cases is explicated in *Reilly v. Ceridian*.[113] In *Reilly*, hackers breached the security systems of the defendant Ceridian Corporation, a payroll processing company.[114] However, no evi-

111. *Attias*, 865 F.3d at 627.
112. *Id.* at 628–29 (citing Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015)).
113. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011). *But see supra* Part V.D.
114. *Id.* at 40.

dence existed that the hackers "read, copied, or understood the data."[115] Plaintiffs were employees of a company that used Ceridian to process its payrolls.[116]

The Third Circuit affirmed the U.S. District Court for the District of New Jersey's decision that plaintiffs lacked Article III standing because they merely alleged a "hypothetical, future injury."[117] Although the U.S. Supreme had not yet decided *Clapper*, the Third Circuit similarly analyzed plaintiffs' injury as resting on — to use *Clapper*'s phrasing — "a highly attenuated chain of possibilities."[118] The Court held that:

> Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.[119]

In contrast to the Seventh and Ninth Circuits, the Third Circuit also dismissed the idea that plaintiffs who spend time, effort, and money on credit monitoring have suffered an injury sufficient to confer Article III standing, finding that "incurred expenses in anticipation of future harm . . . is not sufficient to confer standing."[120] However, in data breach cases where "the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment," the court speculated that Article III standing would exist.[121]

Reilly is not wholly inconsistent with the Seventh Circuit's later decisions in *Remijas* and *Lewert*. In *Remijas*, 9,200 out of 350,000 individuals affected suffered fraudulent charges on their credit cards.[122] In *Lewert*, one named plaintiff, although no oth-

115. *Id.*
116. *Id.*
117. *Id.* at 41.
118. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).
119. *Reilly*, 664 F.3d 38, 42.
120. *Id.* at 46.
121. *Id.* at 45.
122. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

ers, received fraudulent charges.[123] As such, the court could assume in those cases that the hackers "read, copied, and understood" the data as well as would "use such information to the detriment of [the plaintiffs]" as required under the Third Circuit's *Reilly* precedent.[124] Still, the Third Circuit's *Reilly* decision is arguably more stringent than the Seventh Circuit's approach even in those circumstances. For example, in *Lewert*, defendant P.F. Chang's contended that the named plaintiffs never dined at a P.F. Chang's location actually affected by a data breach.[125] In such a situation, it is difficult to see how plaintiffs could show that the P.F. Chang's hackers could have accessed the information as required by *Reilly*.[126] In fact, the Seventh Circuit explicitly held that the question of whether hackers of the defendant actually accessed or could have accessed plaintiff's information is a question of fact to be determined at trial.[127]

2. *The Eighth Circuit*

In *In re SuperValu, Inc.*, hackers accessed individuals' credit card information from computers at grocery stores owned by defendant SuperValu, Inc.[128] Out of the 16 named plaintiffs, however, only one plaintiff actually suffered fraudulent charges.[129] Although the Eighth Circuit ultimately found that the *SuperValu* lawsuit could proceed because one named plaintiff remained who had suffered an actual injury due to the fraudulent charges,[130]

123. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016) (finding that even though only one named plaintiff received fraudulent charges — and the other plaintiff did not — both plaintiffs satisfied Article III standing).

124. *Reilly*, 664 F.3d at 42.

125. *Lewert*, 819 F.3d at 965.

126. *Reilly*, 664 F.3d at 42.

127. *Lewert*, 819 F.3d at 969 ("P.F. Chang's argues that the plaintiffs cannot show causation because their information was never compromised and in any event any fraudulent charges cannot be attributed to its data breach. . . . The latter argument is a theory of defense that P.F. Chang's will be entitled to pursue at the merits phase.").

128. *In re* SuperValu, Inc., No. 16-2378, 2017 WL 3722455 (8th Cir. Aug. 30, 2017).

129. *Id.*, at *2 ("Shortly after the data breach was announced, '[one plaintiff] noticed a fraudulent charge on his credit card statement and immediately cancelled his credit card, which took two weeks to replace.'").

130. *Id.*, at *8 ("Because the complaint contains sufficient allegations to demonstrate that [one named plaintiff] suffered an injury in fact, fairly traceable to defendants' security practices, and likely to be redressed by a favorable judgment, [one named plaintiff] has standing under Article III's case or controversy requirement. . . . Since one named plaintiff has standing to bring suit, the district court erred in dismissing the action for lack of subject matter jurisdiction.").

the court explained that the threat of future identify theft faced by the other 15 named plaintiffs could not satisfy Article III standing.[131] Citing to a report by the Government Accountability Office (GAO), the court found that research on data breaches does "not plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud."[132] Consequently, the Eighth Circuit requires that plaintiffs be able to show fraudulent activity in order to satisfy Article III standing.

3. *The Fourth Circuit*

Beck v. McDonald, decided by the Fourth Circuit, is arguably the most restrictive Article III standing data breach case decided by a federal appellate court.[133] In *Beck*, an individual stole a laptop containing "unencrypted personal information of approximately 7,400 patients, including names, birth dates, the last four digits of social security numbers, and physical descriptors" from a hospital.[134] As a result, the plaintiffs claimed that they had to "frequently monitor their credit reports, bank statements, health insurance reports, and other similar information, purchase credit watch services, and [shift] financial accounts."[135] The Fourth Circuit rejected the theory that plaintiffs could satisfy Article III standing requirements by purchasing credit monitoring without evidence that the stolen data would be used to commit identify fraud:

> Indeed, for the Plaintiffs to suffer the harm of identity theft that they fear, we must engage with the same "attenuated chain of possibilities" rejected by the Court in *Clapper*. In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal

131. *Id.*, at *6.
132. *Id.*, at *5 ("Because the [GAO] report finds that data breaches are unlikely to result in account fraud, it does not support the allegation that defendants' data breaches create a substantial risk that plaintiffs will suffer credit or debit card fraud.").
133. Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).
134. *Id.* at 267.
135. *Id.*

> their identities. This "attenuated chain" cannot confer standing.[136]

Beck therefore further complicates the Article III standing landscape for data breach victims seeking to recover costs incurred when responding to a breach involving their personal information. While evidence that some plaintiffs or putative class members suffered fraudulent charges may bolster the claim that the threat of fraudulent activity to other plaintiffs and putative class members is substantial and imminent, *Beck* holds that such additional evidence is of little importance because it assumes that the hackers will "select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities."[137] Specifically, the Fourth Circuit found that "[e]ven if we credit the Plaintiffs' allegation that 33% of those affected by [the data breach] will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm."[138] The Fourth Circuit's restrictive approach to Article III standing therefore raises the possibility that plaintiffs will have to show that a substantial number of members of the putative class will suffer fraudulent activity; if not, victims of a data breach cannot expect to recover costs associated with credit monitoring and other preventive steps through class action lawsuits.

4. *Approaches from District Court Judges*

Decisions from the U.S. District Court for the Southern District of New York as well as the Eastern District of New York impose restrictive standing requirements, focusing on whether fraudulent charges are reimbursed. In *Hammond v. The Bank of New York Mellon Corporation*, a Southern District judge ruled that the named plaintiffs lacked Article III standing because they had been fully reimbursed for all unauthorized charges resulting from the data breach, thus suffering no injury.[139] More recently,

---

136. *Id.* at 275.
137. *Id.*
138. *Id.* at 275–76.
139. Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (citing People to End Homelessness, Inc. v. Develco Singles Apts. Assocs., 339 F.3d 1, 9 (1st Cir. 2003) (finding that the plaintiff "does not have standing to

an Eastern District judge similarly held that the loss of time and money associated with credit card monitoring cannot satisfy Article III standing under *Clapper*'s imminency requirement;[140] the decision was upheld by the Second Circuit in a non-precedential summary order.[141] In addition to needing a "certainly impending" injury to satisfy *Clapper*, the Eastern District judge held that plaintiffs must also suffer *unreimbursed* charges[142] in order to satisfy the injury-in-fact requirement.[143] This requirement stands in sharp contrast to the approach favored in the Seventh Circuit, in which time, effort, and money spent resolving charges, even if reimbursed, satisfy the injury-in-fact requirement.[144]

Similarly, in *Duqum v. Scottrade*, a judge in the U.S. District Court for the Eastern District of Missouri held that plaintiffs must allege that the stolen data was used — or was intended to be used — to commit identify theft or fraud that would directly affect the plaintiffs themselves.[145] In *Duqum*, hackers gained access to plaintiffs' personal information "for the purpose of building their own competing customer database for marketing and brokering stock transactions" and "to operate a stock price manipulation scheme that amassed millions of dollars."[146] Even though the plaintiffs demonstrated that their personal information was improperly accessed and used, there was no evidence that the improper use harmed the plaintiffs.[147] The judge did not suggest how plaintiffs might demonstrate that hackers intend to use stolen data for nefarious purposes affecting the plaintiffs themselves except by showing fraudulent charges made in their name.

Finally, a judge in the U.S. District Court for the Northern District of Alabama has articulated an approach to Article III

---

pursue its lawsuit because its alleged injuries, to the extent they can be redressed, have already been remedied")).

140. Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015) (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)).

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

142. The requirement that plaintiffs must suffer unreimbursed charges to satisfy injury-in-fact stands in direct contrast to the Seventh Circuit's position. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

143. *Whalen*, 153 F. Supp. 3d at 580.

144. *See Lewert*, 819 F.3d at 967; *Remijas*, 794 F.3d at 693.

145. Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001 (E.D. Mo. July 12, 2016).

146. *Id.* at *1.

147. *Id.* at *6.

standing in data breach cases requiring evidence of data misuse.[148] In *Community Health Systems*, the court found a sufficient injury-in-fact among those plaintiffs that alleged misuse of the stolen data, but explicitly disagreed with the Seventh and Ninth Circuits that Article III standing could be satisfied when plaintiffs could not show unauthorized use of data.[149] The court therefore held that only misuse of data could lead to "certainly impending" future injury, thus satisfying *Clapper*'s imminency requirement.[150] The judge also analyzed the concreteness of plaintiffs' claims in light of *Spokeo*.[151] Similar to its imminency analysis, the court found that only those plaintiffs who alleged misuse of data had suffered a sufficiently concrete injury; the concrete injury may be the time and money spent to resolve fraud as a result of the breach and/or the financial consequences of the fraudulent misuse of the stolen data.[152] An injury is not concrete, however, if it is incurred merely in anticipation of a speculative, future injury.[153]

C. CIRCUIT SPLIT SUMMARY

As evidenced by this survey of court decisions articulating standards of Article III standing in data breach cases, courts have yet to formulate one, or even two, modes of analysis. Instead, some courts appear to find Article III standing's injury-in-fact requirement met whenever plaintiffs assert that their information was exposed to hackers.[154] Other jurisdictions require that "the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment," a high bar for establish-

148. *See In re* Community Health Systems, Inc., Customer Security Data Breach Litigation (MDL 2595), No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016).
149. *Id.* at *9–11.
150. *Id.* at *10–11.
151. *Id.* at *16–17.
152. *Id.* at *15–17.
153. *Id.*
154. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016) ("The plaintiffs 'should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur.'") (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)); *In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2012) ("Although Sony argues that Plaintiffs' allegations are insufficient because none of the named Plaintiffs have alleged that their Personal Information was actually accessed by a third party, neither *Krottner* nor *Clapper* require such allegations.").

ing Article III standing.[155] Even when data breach victims as plaintiffs can prove that their information was stolen and misused, another district court requires that the stolen information be used in a way that causes — or at least has the potential to cause — financial harm to the plaintiffs themselves.[156] Finally, some courts refuse to confer standing absent evidence of *unreimbursed* financial loss.[157]

Notably, the aforementioned cases have almost all primarily focused on the "actual or imminent" harm component of injury-in-fact rather than the concreteness requirement.[158] Even those cases that postdate *Spokeo* do not engage in a thorough concreteness analysis.[159] The *Spokeo* decision, however, adds another layer of complexity for courts analyzing Article III standing in data breach cases because of its requirement that federal courts closely scrutinize the concreteness of injury in addition to imminency and particularization.[160] Judges that make conclusory statements that the risk of future harm satisfies concreteness[161] are unlikely to satisfy the majority of Supreme Court justices who appear intent on ensuring strict compliance with Article III's

155. Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011); *see also In re* Community Health Systems, Inc., Customer Security Data Breach Litigation (MDL 2595), No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016).

156. Duqum v. Scotttrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001 (E.D. Mo. July 12, 2016).

157. Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010); Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 580 (E.D.N.Y. 2015).

158. For a more complete discussion of the imminency requirement in data breach cases, *see* Andrew Braunstein, *Standing Up for Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing*, 24 J.L. & POL'Y 93 (2015) (arguing that *Clapper* announced a heightened injury requirement due to national security concerns that should be inapplicable in the context of data breach litigation).

159. *See* Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., No. 15-3386, 2016 WL 4728027 (6th Cir. Sept. 12, 2016); *In re* Community Health Systems, Inc., Customer Security Data Breach Litigation (MDL 2595), No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016).

160. *See, e.g.*, Kevin M. McGinty & George M. Patterson, *Supreme Court's Spokeo Decision Strengthens Standing Defense For Employers In FCRA And Other Statutory Class Actions*, THE NATIONAL LAW REVIEW (June 3, 2016), http://www.natlawreview.com/article/supreme-court-s-spokeo-decision-strengthens-standing-defense-employers-fcra-and [https://perma.cc/TRH2-82NF] ("*Spokeo*'s explanation of the significance of the concrete injury requirement could prove to be one of the most important passages ever written in the battle against federal minimum damages class action.").

161. *See, e.g.*, *Attias*, 865 F.3d at 627 (stating that "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury" even though none of the plaintiffs alleged identify theft or whether the hackers obtained the type of information necessary to commit fraud).

standing requirements.[162] I now turn to analyze how an emphasis on concreteness in conjunction with imminency is likely to impact data breach litigation going forward.

IV. THE IMPACT OF *SPOKEO* ON DATA BREACH CLAIMS GOING FORWARD

If data breach victims faced an uphill climb establishing injury-in-fact in some jurisdictions prior to *Spokeo*, the Article III standing jurisprudential landscape became more difficult following the 2016 decision. Going forward, plaintiffs not only must satisfy *Clapper*'s articulation of the "imminency" requirement, which may be quite difficult depending on the jurisdiction,[163] but plaintiffs will also have to show that they suffered a "concrete," or "de facto," injury.[164] Stolen data, without evidence of fraud or some other direct impact on the plaintiff, however, will be difficult to classify as "concrete" under the Supreme Court's 2016 *Spokeo* decision. Jurisdictions that have not addressed how stolen or accessed data, without further harm, can constitute a concrete harm[165] are unlikely to persuade the Supreme Court that concreteness of injury has adequately been analyzed. As such, even those jurisdictions that have adopted liberal theories of Article III standing in the context of data breach litigation are likely to have those precedents challenged if and when the Supreme Court decides a data breach case.

In this part, I briefly survey several recent federal court decisions interpreting *Spokeo*'s "concreteness" requirement. Although these decisions do not concern data breaches in particular, they nonetheless shed light on how federal courts are interpreting the *Spokeo* decision with regard to the "concreteness" prong of injury-in-fact. As such, understanding the analysis from these cases can help scholars and litigants better predict the data breach litigation landscape going forward, particularly if and when a data breach case reaches the U.S. Supreme Court. Indeed, the decisions from these cases lead me to predict that the renewed focus

---

162. *See* Spokeo, Inc. v. Robins,136 S. Ct. 1540 (2016) (articulating a strict concreteness requirement); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (articulating a strict imminency requirement).

163. *See supra* Part III.B.

164. *See Spokeo*, 136 S. Ct. at 1548 (citing Black's Law Dictionary 479 (9th ed. 2009)).

165. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

on concreteness will further decrease the ability of data breach victims to have their day in court.

A. "CONCRETENESS" POST-*SPOKEO*

Just one week after the U.S. Supreme Court decided *Spokeo*, a Washington federal district court considered whether a company's violation of federal and state laws prohibiting the use of automatic dialing machines constituted a sufficiently "concrete" injury.[166] In *Booth v. Appstack*, the judge distinguished *Spokeo*, writing that a violation of the Fair Credit Reporting Act (FCRA) in *Spokeo* "was arguably merely procedural and thus non-concrete."[167] In contrast, the judge found that violations of auto-dialer laws "required Plaintiffs to waste time answering or otherwise addressing widespread robocalls."[168] Because plaintiffs were able to show actual injury — loss of time — as a result of the statutory violation, plaintiffs established Article III standing. *Booth* provides support for the proposition that data breach victims suing *under a statute* for loss of time and energy as a result of a data breach would have a stronger argument for satisfying Article III standing than those relying on common law claims.

Federal courts have also determined that unwanted facsimiles, texts, and phone calls that constitute violations of the Telephone Consumer Protection Act (TCPA)[169] are sufficiently concrete injuries due to loss of time. The Northern District of Illinois, in *Brodsky v. Humanadental*, found that although a plaintiff does not suffer financial loss, the fact that the "[f]axes occupied his fax line and machine, used his toner and paper, and wasted his time" showed that the plaintiff was actually injured.[170] The Ninth Circuit has adopted similar reasoning.[171]

166. Booth v. Appstack, Inc., 2016 WL 3030256 at *5 (W.D. Wash. May 25, 2016).
167. *Id.*
168. *Id.*
169. 47 U.S.C. § 227 (2015).
170. Brodsky v. Humanadental Ins. Co., No. 1:10-CV-03233, 2016 WL 5476233, at *11 (N.D. Ill. Sept. 29, 2016).
171. Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037 (9th Cir. 2017) ("Unlike in *Spokeo*, where a violation of a procedural requirement minimizing reporting inaccuracy may not cause actual harm or present any material risk of harm . . ., the telemarketing text messages at issue here, absent consent, present the precise harm and infringe the same privacy interests Congress sought to protect in enacting the TCPA. Unsolicited telemarketing phone calls or text messages, by their nature, invade the privacy and disturb the solitude of their recipients. A plaintiff alleging a violation under the TCPA 'need not allege any additional harm beyond the one Congress has identified.'").

In contrast, however, a recent Eighth Circuit decision found that *Spokeo* effectively overruled the Eighth Circuit's precedent of finding Article III standing whenever statutory rights are violated.[172] In *Braitberg*, the plaintiff sued a cable television provider for storing his personal information past the point for which it was "necessary for the purpose for which it was collected,"[173] a violation of the Cable Communications Policy Act.[174] The court found that the plaintiff failed to allege a concrete injury.[175] While acknowledging that the cable provider "violated a [statutory] duty to destroy personally identifiable information," the Eighth Circuit held that the plaintiff must further identify either a "material risk of harm" or an "economic harm" resulting from the statutory violation in order to satisfy the injury-in-fact requirement post-*Spokeo*.[176]

Most recently, the Ninth Circuit issued its decision in *Spokeo* after the Supreme Court's remand.[177] Following the Supreme Court's instructions to analyze the concreteness of the plaintiff's claims on remand,[178] the Ninth Circuit determined that the plaintiff's injury was sufficiently concrete to satisfy Article III.

In reaching its decision that the *Spokeo* plaintiff satisfied the concreteness requirement, the Ninth Circuit articulated a two-pronged test designed to encapsulate the Supreme Court's holding: "(1) whether the statutory provisions at issue were established to protect [plaintiff's] concrete interests (as opposed to purely procedural rights), and if so, (2) whether the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests."[179] To answer the first question, the Ninth Circuit concluded that Congress' intent in passing the FCRA, the statute at issue in *Spokeo*, was "to protect consumers from the transmission of inaccurate information about

172. Braitberg v. Charter Commc'ns, Inc., No. 14-1737, 2016 WL 4698283, at *4 (8th Cir. Sept. 8, 2016) (citing Hammer v. Sam's East, Inc., 754 F.3d 492, 498–99 (8th Cir. 2014)); Charvat v. Mutual First Federal Credit Union, 725 F.3d 819, 822 (8th Cir. 2013).

173. *Id.* at *1.

174. 47 U.S.C. § 551(e) (2015).

175. *Braitberg*, 2016 WL 4698283, at *4.

176. *Id.* at *4–5; *see also* Hancock v. Urban Outfitters, 830 F.3d 511, 514 (D.C. Cir. 2016) (finding that plaintiffs failed to allege a concrete injury when alleging that defendants violated the Consumer Protection Act by requesting and storing plaintiffs' zip codes in order to complete credit card transactions because plaintiffs did not allege "any invasion of privacy, increased risk of fraud or identity theft, or pecuniary or emotional injury").

177. Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. Aug. 15, 2017).

178. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

179. *Robins*, 867 F.3d at 1113.

them" in consumer reports.[180] Because employment prospects could be hampered by inaccurate reporting, the Ninth Circuit concluded that the FCRA was established to protect concrete interests. In answering the second prong of its test, the Ninth Circuit explained that the type of information that the *Spokeo* plaintiff alleged was inaccurate in his Spokeo credit report — details about his age, marital status, educational background, and employment history — is the exact type of information that employers would consider when deciding whether to hire someone; therefore, "the inaccuracies alleged [are not] the sort of 'mere technical violation[s]' which are too insignificant to present a sincere risk of harm to the real-world interests that Congress chose to protect with FCRA."[181] Consequently, the Ninth Circuit concluded that the plaintiff alleged a sufficiently concrete injury.

At the time of writing, it is unclear whether the *Spokeo* defendant will file a writ of certiorari to the Supreme Court seeking review of the Ninth Circuit's decision on remand.[182] Given the skepticism with which a majority of the Supreme Court views liberal theories of Article III standing,[183] it remains uncertain the degree to which the Ninth Circuit's treatment of the concreteness requirement is conclusive on the issue. For example, in its *Spokeo* decision, although the Supreme Court acknowledged that the "risk of real harm" can sometimes satisfy concreteness, it also explained that the reporting of inaccurate information may result in no harm.[184] Even on remand, it remained unclear who had seen the *Spokeo* plaintiff's inaccurate information and whether that information had an adverse impact on the plaintiff.

B. PREDICTING STANDING IN DATA BREACH CASES FOLLOWING *SPOKEO*

Comparing the facts of the aforementioned post-*Spokeo* decisions with the facts common in data breach cases can help inform a solution that would allow data breach victims a greater likeli-

180. *Id.* (quoting Guimond v. Trans Union Credit Info. Co., 45 F.3d 1329, 1333 (9th Cir. 1995)).

181. *Id.* at 1117.

182. Under Supreme Court Rule 13(1), a petition for a writ of certiorari to review a judgment is timely when it is filed within 90 days after entry of the judgment.

183. *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013); Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

184. *Spokeo*, 136 S. Ct. at 1549–50.

hood of recovering the costs associated with the exposure of their personal information to hackers. As previously discussed, data breach plaintiffs often expend considerable time and money monitoring their credit and resolving fraudulent activity. Plaintiffs often, however, have not suffered a financial loss as the direct result of the data breach. Typically, there is no loss because although hackers have accessed personal information, hackers have not yet used that data to commit fraud.[185] In other cases, the plaintiffs have been reimbursed for any fraudulent activity by either their bank or the company from which the hackers stole plaintiffs' personal information.[186] In this latter category, however, plaintiffs may not be reimbursed to the extent necessary to adequately compensate for their expenses or may have to expend additional resources beyond those that the company will reimburse.[187]

In *Spokeo*, the Supreme Court recognized that "intangible" injuries can be concrete and that the "risk of real harm can[] satisfy the requirement of concreteness."[188] The Court's decision therefore supports the proposition that data breach plaintiffs may be able to claim that the loss of time due to credit monitoring is a "concrete injury."[189] Nonetheless, plaintiffs relying on such an interpretation of *Spokeo* will face two significant hurdles in making such a comparison.

First, the plaintiffs in *Brodsky* and *Booth*, the post-*Spokeo* cases discussed above,[190] expended time and effort *in response to* actions taken by the defendant. In *Brodsky*, the defendant sent unwanted faxes to the plaintiff; in *Booth*, the defendant placed unwanted telephone calls.[191] In contrast, data breach plaintiffs who expend time, effort, and money in monitoring their credit and identity do so preemptively and in direct response to the ac-

185. *See* Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016).

186. *See, e.g.*, Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015).

187. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x. 384, 386 (6th Cir. 2016) (explaining that defendant-company only offered one-year of free credit monitoring).

188. *Spokeo*, 136 S. Ct. at 1549.

189. *See* Brodsky v. Humanadental Ins. Co., No. 1:10-CV-03233, 2016 WL 5476233 (N.D. Ill. Sept. 29, 2016); Booth v. Appstack, Inc., 2016 WL 3030256 (W.D. Wash. May 25, 2016).

190. *See supra* Part IV.A.

191. *See Brodsky*, 2016 WL 5476233; *Booth*, 2016 WL 3030256.

tions of a third-party hacker, not the defendant-company.[192] Courts must therefore speculate as to the likelihood that an unknown third party not before the court will one day harm the plaintiffs. Unlike faxes and telephone calls that already occurred, hackers may never understand or use the stolen data.[193] Alternatively, plaintiffs may have great difficulty establishing the intent of the hackers as required by some jurisdictions.[194] To allow data breach plaintiffs to claim a "concrete" injury as a result of loss of time in monitoring their credit therefore arguably permits plaintiffs to "manufacture" standing. The Supreme Court, however, has explicitly rejected such an approach to injury-in-fact: "[Plaintiffs] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[195]

On the other hand, some data breach lawsuits feature plaintiffs who have already suffered fraudulent activity.[196] It stands to reason that in these circumstances, plaintiffs have alleged a sufficiently "concrete" injury when they claim to have suffered loss of time in resolving such charges because they expended resources in response to an occurrence that already happened.[197] And certainly when plaintiffs suffer *unreimbursed* financial loss as a result of a data breach, a concrete injury is almost definitely pre-

192. Plaintiffs can argue that the negligence of the defendant-company, not necessarily the actions of the hackers, creates the need to monitor their credit and identity. However, even the courts adopting the most liberal versions of standing in data breach cases have viewed the "injury" as the risk of fraudulent activity in the future rather than the mere fact that personal information was exposed. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016) (identifying the injury as the imminent harm of fraudulent activity); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (identifying the injury as the "credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.").

193. This concern may be mitigated when there is evidence that some members of the putative class saw fraudulent activity, but note that some jurisdictions require evidence that the majority of the putative class will be affected by fraudulent activity, not just some individual plaintiffs. *See* Beck v. McDonald, 848 F.3d 262, 275–76 (4th Cir. 2017) ("Even if we credit the Plaintiffs' allegation that 33% of those affected by [the data breach] will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm.").

194. *See* Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); *see also* Khan v. Children's Nat'l Health Sys., No. CV TDC-15-2125, 2016 WL 2946165, at *5 (D. Md. May 19, 2016).

195. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013).

196. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

197. *See* Brodsky v. Humanadental Ins. Co., No. 1:10-CV-03233, 2016 WL 5476233 (N.D. Ill. Sept. 29, 2016); Booth v. Appstack, Inc., 2016 WL 3030256 (W.D. Wash. May 25, 2016).

sent under even the strictest interpretation of the "concreteness" requirement because the plaintiffs have lost money as a result of the data breach caused by the defendant company's lack of sufficient data security measures. Nonetheless, only allowing victims of data breaches to access court in these circumstances will leave many victims in the position of expending time and money on credit monitoring and similar services without being able to recover incurred costs.

Second, *Spokeo* — as well as *Brodsky* and *Booth* — concerned alleged violations of federal statutes. An important aspect of the injury, therefore, was that the defendant allegedly breached its duty to the plaintiffs *as defined in the statute*. As previously mentioned, data breach plaintiffs typically assert claims of negligence, breach of implied contract, negligent infliction of emotional distress, and other common law claims against the defendant companies that allegedly failed to adequately protect their information from access by hackers.[198] There is no comprehensive federal statute dealing with data breaches or regulating companies' duties to individuals from whom they collect and store personal information. As a result, sufficient concreteness of injury is even more difficult to identify because the harm is not defined or specified by Congress.

It stands to reason, then, that were Congress to identify and define specific harms resulting from data breaches as well as duties owed by companies to individuals whose information they store, data breach victims would have a stronger claim to Article III standing. If Congress creates an explicit duty to safeguard collected information and penalties for falling short of that duty, the injury inflicted in a data breach would be the breach of that duty rather than simply a risk of future injury resulting from hackers' improper use of data.

198. *See* Elizabeth T. Isaacs, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 543–50 (2015) (detailing the faults associated with the frequently asserted common law-based claims in data breach cases); Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 231 (2015); *see also, e.g.*, *Remijas*, 794 F.3d at 688; *Reilly*, 664 F.3d at 38; Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010). *But see* Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (basing claims primarily on the Privacy Act because defendants were operators of a government-run facility).

V. A STANDING SOLUTION: STATUTORY STANDING

As previously discussed, under the current state of Article III standing jurisprudence, many data breach victims will not be able to recover losses they suffer as a result of companies' failures to safeguard their personal information. Once notified that their data has been exposed, it is both rational and advisable for data breach victims to monitor their credit or identity in order to prevent fraud. Indeed, companies routinely advise data breach victims to monitor their financial information in the wake of a data breach.[199] Nevertheless, only the Sixth, Seventh, and Ninth Circuit U.S. Courts of Appeals have articulated a liberal theory of standing in data breach cases that allows victims to recover costs — financial and otherwise — associated with monitoring.[200] The Seventh and Ninth Circuits, however, have not yet reexamined their standing analyses in light of the recent *Spokeo* decision on the importance of concreteness in any Article III standing inquiry, and the Sixth Circuit did not cite to *Spokeo* in its recent concreteness analysis.[201] Thus it is possible that even in those jurisdictions, plaintiffs will soon face greater hurdles in establishing standing in data breach cases.

In order to solve the challenges data breach victims encounter as a result of the previously described Article III standing doctrines, I argue that Congress should enact a statute that comprehensively regulates data breaches and grants victims certain statutory rights and remedies.[202] While some legal academics

---

199. *See, e.g.*, Nick Bilton & Brian Stelter, *Sony Says PlayStation Hacker Got Personal Data*, N.Y. TIMES (April 26, 2011), http://www.nytimes.com/2011/04/27/technology/27playstation.html [https://perma.cc/2MRZ-4BBP].

200. *See, e.g.*, *Remijas*, 794 F.3d at 688; *Krottner*, 628 F.3d at 1139.

201. To add to this point, Braunstein argues that lower courts have misapplied *Clapper* when denying Article III standing in data breach cases, arguing that the "loss of data itself" is an "actual" injury; he asserts that the "true injury the Court looked for in *Clapper* was the 'interception' of the plaintiffs' communications. . . . [T]he interception itself would have been enough if the plaintiffs had been able to demonstrate it had actually occurred." *See* Andrew Braunstein, *Standing Up for Their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing*, 24 J.L. & POL'Y 93, 123–124 (2015). Even if federal courts would accept Braunstein's characterization of *Clapper*'s proper application of the imminency requirement in data breach cases, Braunstein nevertheless fails to consider that "loss of data" alone would likely not be considered a sufficiently "concrete" injury, especially after *Spokeo*.

202. In 2014, Congress enacted several laws relating to data breaches affecting government agencies, but failed to act on several bills related to private sector data breaches. *See* Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the*

and commentators urge the U.S. Supreme Court to reexamine its Article III standing jurisprudence,[203] such calls are likely to fall on deaf ears considering the Court's trend toward requiring an increasingly exacting Article III standing inquiry before plaintiffs can proceed in federal courts.[204] However, the Court has long recognized that "Congress may 'elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.'"[205] Were Congress to enact a properly fashioned statute regulating data breaches, the result would be "a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute."[206] A statutory solution therefore offers data breach victims greater access to federal court without requiring the Court to revisit its Article III jurisprudence.

In this part, I first detail how Article III standing based on a statute's right of action removes many of the separation of powers concerns federal courts have with broadly conferring standing in the absence of such a statute. I then briefly describe the limits of statutory standing. I proceed with a proposed framework for potential data breach legislation that would ensure that data breach victims gain greater access to federal courts in order to

---

2013 Mega Breaches and Beyond, 24 COMPETITION: J. ANTI. & UNFAIR COMP. L. SEC. ST. B. CAL. 229, 238–41 (2015).

203. *See, e.g.*, Michael B. Jones, *Uncertain Standing: Normative Applications of Standing Doctrine Produce Unpredictable Jurisdictional Bars to Common Law Data Breach Claims*, 95 N.C. L. REV. 201, 220–224 (2016) (arguing that *Clapper*'s "certainly impending" injury should not be applied in disputes between private parties); 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, 1492–96 (2016) (arguing that a "straightforward Article III standing analysis is practically flawed" when applied to data breach cases and that courts should adopt "a stricter, factor-based standing analysis of increased risk that merges elements from the standing and damages inquiries"); Corey Varma, *The Presumption of Injury: Giving Data Breach Victims "A Leg to Stand on*," 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 301, 314–316 (2016) (suggesting a framework in which there is a rebuttable presumption of injury in data breach cases); Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way Towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2016 COLUM. BUS. L. REV. 544 (2016) (arguing that the liberal standing approach favored by the Seventh Circuit in *Remijas* should be adopted).

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

205. *Spokeo*, 136 S. Ct. at 1549 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)); *see also Lujan*, 504 U.S. at 580 (Kennedy, J., concurring) ("Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before.").

206. Warth v. Seldin, 422 U.S. 490, 514 (1975).

recover reasonable expenses sustained in the response to a breach while also staying within the limits on statutory standing prescribed by the Supreme Court. Finally, I conclude with a discussion of a recent Third Circuit decision that demonstrates the viability of a statutory solution in the data breach context.

A. THEORY BEHIND STATUTORY STANDING

As previously discussed, Article III standing doctrine has its roots in the theory of separation of powers.[207] Traditionally, federal courts have been wary of intruding upon the proper role of the legislative branch by allowing individuals to pursue rights in court that were not an established part of the common law. To do so would allow federal courts to "make" law, which is properly the role of the legislative branch. Statutory standing, however, offers a theoretical solution to the separation of powers dilemma encountered by courts in cases such as those dealing with data breaches: "By deferring the authority to create a private right of action to Congress or state legislatures, the judiciary stays within its proper role in the American system of government."[208] By enacting a statute granting victims of data breaches certain rights and remedies, Congress therefore absolves the judiciary of the need to fashion new duties that were previously unrecognized by either the common law or prior congressional enactments.

B. LIMITS TO STATUTORY STANDING[209]

While Congress can "elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law,"[210] the Supreme Court has recognized that Congress cannot give individuals a "blank check" to vindicate rights merely because they are spelled out in statutes. Any law that purports

---

207. *Supra* Part II.

208. Patricia Cave, *Giving Consumers A Leg to Stand on: Finding Plaintiffs A Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U.L. REV. 765, 789 (2013).

209. For a more thorough examination of the Court's decisions regarding Article III standing provided by statutes, *see* John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219 (1993).

210. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)).

to create a private right of action that bypasses Article III standing requirements is unconstitutional.[211]

Most notably, in *Lujan*, the Court held that although the Endangered Species Act[212] created a right of action for the plaintiffs, the plaintiffs nevertheless failed to establish Article III standing. The Endangered Species Act states that "any person may commence a civil suit on his own behalf . . . to enjoin any person, including the United States and any other governmental instrumentality or agency . . . who is alleged to be in violation of any provision of this chapter."[213] Generally, the Endangered Species Act prohibits the U.S. government from taking actions that would cause harm to endangered animal species.[214] The plaintiffs — who alleged that the Secretary of the Interior violated the Act by promulgating a regulation stating the law applied only to agency actions taken *within* the United States — satisfied the requirements under the statute.

Justice Scalia, writing for the majority, found that the plaintiffs lacked an injury-in-fact as required by Article III.[215] The plaintiffs alleged injury because they "had visited" foreign countries in which endangered animals may have been affected as a result of the Interior Department's new regulation; plaintiffs also claimed that they planned to visit those foreign countries (and view the endangered species) in the future. Crucially, however, plaintiffs conceded that they did not have any specific travel plans.[216] The Court held that "[s]uch 'some day' intentions — without any description of concrete plans, or indeed even any specification of *when* the some day will be — do not support a finding of the 'actual or imminent' injury that our cases require."[217]

In addition to questioning the imminency of injury, the Court also questioned the concreteness of the plaintiffs' injury, analyzing the constitutionality of "generalized-grievance" statutes, which allow any citizen to sue in federal court in order to enforce provisions of a statute. Justice Scalia wrote:

---

211. *See* John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1226–1229 (1993).
212. 16 U.S.C. § 1531 (2016).
213. 16 U.S.C. § 1540(g) (2016).
214. 16 U.S.C. § 1536(a)(2) (2016); *see also* Lujan, 504 U.S. at 558.
215. *Lujan*, 504 U.S. at 566–67.
216. *Id.* at 563–564.
217. *Id.* at 564.

> If the concrete injury requirement has the separation-of-powers significance we have always said, the answer must be obvious: To permit Congress to convert the undifferentiated public interest in executive officers' compliance with the law into an "individual right" vindicable in the courts is to permit Congress to transfer from the President to the courts the Chief Executive's most important constitutional duty, to "take Care that the Laws be faithfully executed." It would enable the courts, with the permission of Congress, "to assume a position of authority over the governmental acts of another and co-equal department," and to become "virtually continuing monitors of the wisdom and soundness of Executive action."[218]

The Court reiterated, however, that "[t]he . . . injury required by Art. III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[219]

Justice Kennedy wrote separately in *Lujan*, noting that the decision stands for the proposition that "there is an outer limit to the power of Congress to confer rights of action," calling it "a direct and necessary consequence of the case and controversy limitations found in Article III."[220] As such, it is clear that a broadly written statute seeking to confer standing on plaintiffs following a data breach may violate the Article III principles enunciated in *Lujan*. Nonetheless, a data breach statute can successfully be distinguished from the facts in *Lujan*. For example, the ESA provided that "any person" could sue the U.S. government for an alleged violation.[221] A data breach statute, in contrast, need only give the right to sue to those specific individuals whose personal information is exposed. Additionally, in *Lujan*, the plaintiffs had no plans to view the endangered species; the injury to the plaintiffs themselves was highly speculative. In the data breach context, most plaintiffs expend resources in response to a data breach; at least one injury, therefore, has already occurred at the time a lawsuit is filed. In the next section, I elaborate on these distinctions and craft a hypothetical data breach statute that

---

218. *Id.* at 577 (internal citations omitted).
219. *Id.* at 578 (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)).
220. *Id.* at 580 (Kennedy, J., concurring).
221. 16 U.S.C. § 1540(g).

ameliorates the concerns raised by the facts and legal issues in *Lujan* as well as *Spokeo* and *Clapper*.

C. DESIGNING A STATUTE FOR DATA BREACH VICTIMS

Before proceeding to consider the specific provisions of a hypothetical data breach statute and how the law would satisfy Article III standing requirements, I will briefly address the desirability of a data breach statute as a matter of policy. First, as with any new regulation of businesses, there is an uncertain, but likely, economic impact as a result of companies making changes in order to comply with the new law. Costs of compliance may be passed on to consumers. Conceding that there will be costs associated with compliance, the costs likely will not be much higher than the status quo. Instead, costs will simply be shifted and more front-loaded.

As discussed, each federal jurisdiction takes a different approach to Article III standing in data breach cases.[222] Consequently, there is great uncertainty about the liability and financial exposure as a result of a data breach, especially because of class actions. Companies must already factor in such uncertainty when considering the costs of their data security practices. Moreover, companies presently bear the costs of extensive litigation as a result of a data breach. A data breach statute provides companies with the benefit of a clearer legal landscape, reducing uncertainty and minimizing the quantity and scope of litigation. A statute is also likely to minimize forum shopping because plaintiffs are likely encouraged by the current legal regime to file data breach class actions in those jurisdictions with the most liberal standing precedents assuming other jurisdictional requirements are met. Finally, I note that the companies least likely to suffer a data breach are the ones with the best security practices and are therefore the ones least likely to have to institute major changes following the statute's enactment.

Second, businesses and policymakers will likely argue that consumers assume a certain degree of risk when providing companies with their personal information. As a result, companies should not be required to cover the costs consumers incur following a data breach, particularly when hackers do not misuse data.

---

222. *Supra* Part III.

Knowing that they provided their personal information to third parties, the argument goes, reasonable customers would monitor their personal accounts regardless of notification of a data breach. Legislation, however, frequently re-allocates risks. The relevant question for policymakers must be which parties are best able to bear the risk. In the present context, it would be nearly impossible for individuals to participate in the modern economy without sharing personal information on a near-daily basis. Guarding against fraud and identity theft is more burdensome than simply checking one's credit card statement every few days; it often requires the purchasing of costly credit monitoring services and other fraud-prevention measures. Many individuals, however, would not consider it reasonable to pay a monthly or annual fee when the likelihood of utilizing such a service is relatively low; most individuals, after all, will not be affected by a data breach in any given year. Consequently, while acknowledging the costs associated with a new data breach law, I argue that a balancing of the costs and benefits weigh strongly in favor of a data breach statute. I now turn to considering what provisions to include in a hypothetical data breach statute and how they would satisfy Article III standing.

In order to sufficiently and successfully expand the scope of redressable injuries resulting from data breaches, a hypothetical congressional enactment on data breaches (the Statute) will have to be carefully fashioned. As previously discussed, the Statute cannot confer Article III standing absent a sufficiently "concrete" injury, and it must also comport with the other requirements of Article III standing.[223]

At its core, I suggest that the Statute should create a duty owed to individuals by companies that obtain and store individuals' private information. Guided by the latest data security research available at the time of its drafting, the Statute would set minimum, but stringent, standards for data security practices. The Statute would mandate that companies that experience a data breach notify[224] those individuals whose information may

223. *Supra* Part V.B.

224. Forty-eight states currently require institutions to notify individuals when data breaches occur, but there is no federal statute with a similarly broad notification requirement. *See* Pam Greenberg, *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Apr. 12, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/2WCF-93UH].

have been exposed to — or accessed by — hackers.[225] Additionally, the Statute would allow the notified victims of a data breach to expend "reasonable" resources to protect their financial information and/or identity if the company affected by the breach does not provide those services for free. The Statute would require the company either to provide free credit monitoring services to those affected by the data breach or to fully reimburse victims for reasonable credit monitoring expenses as well as any fraudulent charges that can be traced to the breach. Companies that do not follow the Statute's requirements — for example, by providing insufficient reimbursement — would be subject to liability, and crucially, the Statute would allow plaintiffs to pursue their claims to recover associated costs in federal court.

1. *Particularization*

A statutorily-created right of action for data breach victims must ensure that only those individuals actually affected by the data breach are allowed to sue as plaintiffs.[226] In order to satisfy particularization, the Statute should state that all companies that obtain and store individuals' personal information owe those individuals a duty to keep such information safe and secure from access by third parties. If a hacking occurs, individuals whose information was exposed to the third party can adequately show that the offending company breached a duty owed to them *in particular*.[227] Moreover, if a company knows that it was hacked in general, but does not have information about which particular individuals' personal information was exposed, the Statute would require a company to immediately investigate and identify the scope of the breach.

---

225. For example, in the Yahoo! data breach discussed above, *infra* Part I, individuals whose information was exposed were not informed of the data breach for two years, even though evidence suggests Yahoo! knew of the breach for at least several months before notifying its users. *See* Harriet Taylor, *Yahoo CEO Mayer knew about data breach in July: Report*, CNBC (September 23, 2016, 3:51 PM), http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html [https://perma.cc/969M-KECU]; Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (September 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html?_r=1 [https://perma.cc/G5RK-YSTE].

226. For a discussion on particularization, *see supra* Part II.B.1.

227. *See* Elizabeth T. Isaacs, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 555 (2015).

2. *Imminent or Actual Injury*

In order to ensure that the Statute only allows individuals who have suffered an "actual or imminent" injury to have standing to sue, the law should explicitly allow individuals whose information has been exposed in a data breach to expend "reasonable" time, money, and effort protecting against identity theft and credit card fraud. Elizabeth Issacs, in a similar attempt to formulate a hypothetical statute regulating private suits against companies that suffer data breaches, argues that the law should incorporate the Third Circuit's requirement from *Reilly* that individuals be able to show that hackers actually understood — not merely accessed — data and intended to "commit future criminal acts."[228] Issacs' formulation, while adding strength to the argument that her hypothetical statute would only protect "imminent or actual" injuries, would leave too many victims of data breaches unable to recover reasonable expenses associated with protecting against identify theft and/or fraudulent credit charges. In many instances, it may be unclear whether the hackers understood the information,[229] and hackers may wait many months or years before using that data to commit criminal acts.[230]

Rather than a reformulation of *Reilly*, the Statute should go further to protect victims of data breaches. The Statute can accomplish this goal by mandating that companies reimburse individuals for reasonable expenditures as well as fraudulent charges resulting from a data breach. If affected companies fail to adequately reimburse individuals, hypothetical plaintiffs have suffered an "actual" injury, not merely a procedural one or one that may or may not occur in the future. By providing for such a provision in the Statute, the "actual" injury sufficient to confer statutory standing under Article III does not occur when the stolen

228. *Id.*; *see also* Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

229. Isaacs notes that the Third Circuit test, incorporated in a statute, need not be a rigid one. She suggests, for example, that the fact that the information was not encrypted may be enough for plaintiffs to show that the data was "understood" by hackers. Nonetheless, such an analysis assumes some level of technological sophistication of hackers, which the hackers may surpass. *See* Elizabeth T. Isaacs, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 555 (2015).

230. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007) (finding that "stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.").

data is actually used by a third-party hacker. Instead, the injury occurs when the company fails to adequately safeguard individuals' information, and individuals, in response, spend unreimbursed resources protecting against further adverse consequences. By moving the "injury" forward in time, the Statute bypasses much of the conflicting doctrines coming out of the circuit split on Article III standing in data breach cases.[231] Moreover, while plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending,"[232] Congress can, and does, create new duties and private rights of action.[233] These statutes, moreover, can impose penalties — such as requiring companies to pay actual damages — when companies breach those duties.[234] Requiring reimbursement of mitigation expenses, therefore, can be viewed as simply defining an injury and requiring violators to pay "actual damages." Consequently, if Congress requires companies affected by a data breach to reimburse mitigation expenses for consumers and the company fails to do so, data breach victims suffer an actual injury.

3. *Concreteness*

Finally, as discussed at length in *Spokeo*,[235] a statute can only confer Article III standing if the injury is sufficiently "concrete," or "de facto." In other words, the injury cannot simply be procedural. The plaintiff must show some damage he or she has personally suffered; the mere fact that the defendant did not comply with the relevant statute is insufficient. Under the data breach

231. *See supra* Part III.

232. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013).

233. *See, e.g.*, Lujan v. Defs. of Wildlife, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring) ("[W]e must be sensitive to the articulation of new rights of action that do not have clear analogs in our common-law tradition. . . . Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before . . .").

234. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681n(a) (2016) ("Any person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of — . . . any actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000."); Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3) ("A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State — . . . an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater.").

235. *Supra* Part II.B.2.

Statute, plaintiffs would have to show that that they spent time and money protecting against fraudulent activity as a direct result of a data breach in which their information was exposed to hackers. Moreover, they would have to show that the company did not reimburse them for such charges, or did not reimburse a "reasonable" amount, as required by the Statute. By alleging such facts, plaintiffs would show that their injury was "de facto" because they personally lost time and money, and the Statute gave them a right to be reimbursed for those mitigation expenses. Moreover, a failure to reimburse reasonable costs would be exactly the type of injury that Congress intended to remedy in passing the Statute and would be more than a mere procedural violation that does not result in actual harm.[236]

The injury suffered by data breach victims under the Statute would therefore differ significantly from the injury claimed by the *Spokeo* plaintiff. Although the defendant-company Spokeo violated the FCRA by reporting false information about an individual, it was unclear whether the *Spokeo* plaintiff could show harm or risk of harm because it was uncertain who may have seen the false information or whether those who saw the false information treated the *Spokeo* plaintiff negatively because of it.[237] The *Spokeo* plaintiff sought statutory penalties due to the FCRA violation, but could not demonstrate actual damages due to an inability to show how the incorrect information harmed or could harm him. In contrast, data breach victims could clearly show costs — i.e., actual damages — incurred as a result of a data breach.

4. *Summary*

The hypothetical data breach Statute outlined here would allow data breach victims to recover mitigation costs incurred in the aftermath of a data breach while avoiding the standing pitfalls faced by the *Lujan*, *Clapper*, and *Spokeo* plaintiffs. By authorizing only those individuals whose information is exposed in a data breach to sue, the Statute differs from the law at issue in

236. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016) ("A violation of one of the FCRA's procedural requirements may result in no harm. . . . [N]ot all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.").

237. *See* Spokeo, 136 S. Ct. at 1546.

Lujan, which allowed "any person" to sue. Unlike the alleged injuries in *Clapper* and *Lujan*, which had not yet occurred, the injury for which data breach plaintiffs would sue is not a speculative, future injury, but one that already occurred: the uncompensated expenditure of time, money, and other resources that companies affected by a data breach would be required by the Statute to provide to victims. Finally, the injury would be concrete, not merely procedural, because plaintiffs could show loss of resources connected to the data breach. This injury contrasts with the facts of *Spokeo*, in which it was unclear whether the plaintiff suffered any actual loss or damage due to the defendant-company's failure to comply with the relevant law.

Further, the Statute overcomes the obstacles faced by most data breach victims today. Because the common law does not treat loss of personal information or mitigation expenses as an injury, data breach plaintiffs and courts must presently view the injury in data breach cases to be misuse of personal information by hackers. However, if Congress creates a duty for companies to safeguard personal information as well as reimburse individuals affected by a breach, the injury in a data breach is not only the misuse of data, but also the failure of the company to comply with federal law. The statutory violation would result in a particularized, concrete, and actual injury, satisfying the demands of Article III.

D. USING A STATUTORY SOLUTION TO OVERCOME STANDING CHALLENGES: A CASE STUDY

On January 20, 2017, the U.S. Court of Appeals for the Third Circuit released its decision in *Horizon Healthcare Services*.[238] The facts in *Horizon* are similar to the data breaches discussed earlier.[239] Laptops containing the personal information of 839,000 Horizon members were stolen. Horizon offered one year of credit monitoring, which plaintiffs claimed was inadequate. One of the 839,000 victims claimed a third party fraudulently submitted a tax return in his name and attempted, unsuccessfully, to use his credit card.[240] Unlike the previously discussed data

238. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625 (3d Cir. 2017).
239. *See supra* Part III.
240. *Horizon*, 846 F.3d at 630.

breach cases, however, the victims in the Horizon breach could (and did) sue under the Federal Credit Reporting Act (FCRA) because Horizon is a consumer reporting agency.[241]

The district court dismissed plaintiffs' claims against Horizon, finding a lack of Article III standing. Similar to *Spokeo*'s emphasis on concreteness, the district court found that plaintiffs had to identify some "specific harm" beyond the mere alleged statutory violation arising out of Horizon's failure to keep personal information confidential as required by the FCRA.[242] The district court also addressed the standing of the one plaintiff who had a fraudulent tax return submitted in his name, concluding that the fact that only one out of 839,000 victims suffered harm "demonstrate(s) that [the plaintiff's] identity was stolen through other means."[243] Such analysis bolsters the observation that just because some plaintiffs are affected by fraudulent activity does not necessarily strengthen the claim of Article III standing for other plaintiffs.[244]

The Third Circuit reversed the district court, finding that the plaintiffs satisfied all elements of Article III standing. Addressing the claims against Horizon in light of the Supreme Court's *Spokeo* decision, the Third Circuit found that the plaintiffs "do not allege a mere technical or procedural violation of FCRA. They allege instead the unauthorized dissemination of their own private information — the very injury that the FCRA is intended to prevent. There is thus a de facto injury that satisfies the concreteness requirement for Article III standing."[245]

---

241. Specifically, the plaintiffs alleged that Horizon violated the FCRA's requirement that agencies adopted "reasonable procedures" to safeguard personal information. *Id.* at 631; *see also* 15 U.S.C. § 1681(b) (2016).

242. *Horizon*, 846 F.3d at 634; *In re* Horizon Healthcare Servs., Inc. Data Breach Litig., No. CIV.A. 13-7418 CCC, 2015 WL 1472483, at *5 (D.N.J. Mar. 31, 2015) ("Plaintiffs . . . do not allege any specific harm as a result of Horizon's stolen laptops and therefore may not rest on mere violations of statutory and common law rights to maintain standing.").

243. *Horizon*, 2015 WL 1472483, at *7. Alternatively, the district court found that even if the fraudulent tax return "was 'fairly traceable' to [the Horizon data breach], [the] claim must fail at the third element of standing: redressability [because the plaintiff] admits receiving his tax refund."). *Id.* at *8.

244. *See also* Beck v. McDonald, 848 F.3d 262, 275–76 (4th Cir. 2017) ("Even if we credit the Plaintiffs' allegation that 33% of those affected by [the data breach] will become victims of identity theft, it follows that over 66% of veterans affected will suffer no harm. This statistic falls far short of establishing a 'substantial risk' of harm.").

245. *Horizon*, 846 F.3d at 640 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549).

Horizon demonstrates how a relevant statute can strengthen the Article III standing arguments of data breach victims. The Third Circuit had previously articulated a strict interpretation of Article III standing requirements in *Reilly*, a case in which the data breach victims sued under state common law claims.[246] In *Horizon*, the Third Circuit reiterated the position that data breach plaintiffs suing under state law are unlikely to satisfy Article III standing requirements absent some demonstrable financial injury:

> We are not suggesting that Horizon's actions would give rise to a cause of action under common law. No common law tort proscribes the release of truthful information that is not harmful to one's reputation or otherwise offensive. But with the passage of FCRA, Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself — whether or not the disclosure of that information increased the risk of identity theft or some other future harm.[247]

Crucially, even though the dissemination of personal information due to a failure to reasonably safeguard data may be an "intangible" injury, the Third Circuit found that since the harm that the statute seeks to remedy "has a close relationship to a harm [i.e. invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts . . . we have no trouble concluding that Congress properly defined an injury that 'give[s] rise to a case or controversy where none existed before.'"[248] The Third Circuit summarized the *Horizon* rule regarding Article III statutory standing rule most recently in a July 2017 decision regarding the Telephone Consumer Protection Act (TCPA):

> When one sues under a statute alleging "the very injury [the statute] is intended to prevent," and the injury "has a close relationship to a harm . . . traditionally . . . providing a basis for a lawsuit in English or American courts," a concrete injury has been pleaded. We do not, and need not, conclude

246. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); *supra* Part III.D.
247. Horizon, 846 F.3d at 639.
248. *Id.* at 639–640 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).

> that intangible injuries falling short of this standard are never concrete. Rather, we simply observe that all intangible injuries that meet this standard are concrete.[249]

The *Horizon* decision therefore adds strength to the argument that Congress can pass legislation that creates a duty for companies to safeguard private information. The FCRA only applies to consumer reporting agencies, and thus provides the vast majority of data breach victims no protection. Nonetheless, as discussed in *Horizon*, Congress can elevate such injuries to the status of cognizable injuries that can satisfy Article III standing.[250] Moreover, a statutory solution to the Article III standing issues faced by data breach victims would likely survive legal scrutiny because data breaches are related to invasion of privacy, a tort that the common law recognizes, and the exact harm that Congress would intend to remedy in passing a data breach statute would be inadequate compensation as a result of individuals expending resources in response to a data breach.[251] Just as the FCRA and TCPA allow individuals to recover actual damages from those companies that violate congressionally-created duties that relate to common law duties, the Statute would similarly allow the recovery of actual damages — in the form of reasonable mitigation expenses — in response to a data breach.

VI. CONCLUSION

If recent trends are any indication, the frequency and severity of data breaches of major companies in the United States will only increase in the future.[252] Under current law, however, indi-

---

249. Susinno v. Work Out World Inc., 862 F.3d 346, 351 (3d Cir. 2017) (internal citations omitted).

250. *See also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992) (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)) ("The . . . injury required by Art. III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'").

251. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."); *Susinno*, 862 F.3d at 350 (explaining that the TCPA violation at issue has a close relationship to traditional claims for invasion of privacy and nuisance); Horizon, 846 F.3d at 638 (explaining that "'unauthorized disclosures of information' have long been seen as injurious").

252. *See, e.g.*, Nate Lord, *The History of Data Breaches*, DIGITAL GUARDIAN (Oct. 12, 2016), https://digitalguardian.com/blog/history-data-breaches [https://perma.cc/E3CA-DPH9]; *see also* Heather Landi, *Report: Healthcare Data Breaches Continue at Alarming*

viduals whose personal information has been accessed cannot always recover the costs of such a breach. Some jurisdictions — such as the Sixth, Seventh, Ninth, and D.C. Circuits — favor liberal Article III standing doctrines, allowing data breach victims to sue companies that fail to adequately protect their information. Many other jurisdictions, however, impose more stringent requirements, and only allow victims to sue when they can prove their personal information has already been fraudulently misused[253] or, in an extreme case, can show actual, unreimbursed financial loss.[254] The recent *Spokeo* decision, moreover, is likely to make it even more difficult for data breach victims to recover for losses as courts must now more closely scrutinize whether plaintiffs allege a sufficiently "concrete" injury, an inquiry that many lower courts have so far largely avoided in data breach litigation.

In order to ensure that data breach victims can recover losses they suffer from responding to a data breach implicating their personal information, I have suggested that Congress enact a comprehensive statute regulating data breaches that includes a private right of action.[255] My theoretical statute would: (1) require companies to notify individuals whose information may have been accessed by hackers; (2) allow individuals whose information may have been accessed to expend "reasonable" resources in order to prevent credit card or identity fraud; (3) require companies to reimburse individuals for those reasonable expenses; and (4) provide for a private right of action for individuals to sue companies that do not cover or immediately reimburse their reasonable mitigation expenses. Such a statute would overcome many of the existing issues with Article III standing in data breach cases by creating a duty owed by companies in possession of personal information to those whose personal information they store. A breach of this duty, then, would constitute an "actual," "concrete," and "particularized" injury, satisfying the requirements for injury-in-fact under the Court's Article III standing

---

Pace in Second Half of 2016, HEALTHCARE INFORMATICS (Oct. 17, 2016), https://www.healthcare-informatics.com/news-item/cybersecurity/report-healthcare-data-breaches-continue-alarming-pace-second-half-2016 [https://perma.cc/93H9-VNKT].

253. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011); *In re* Community Health Systems, Inc., Customer Security Data Breach Litigation (MDL 2595), No. 15-CV-222-KOB, 2016 WL 4732630 (N.D. Ala. Sept. 12, 2016).

254. Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015).

255. *Supra* Part V.C.

jurisprudence as evidenced in the Third Circuit's 2017 *Horizon* decision.

The current jurisprudential regime surrounding Article III standing in data breach litigation results in unfair outcomes for victims of data breaches. Due to no fault of their own, individuals' personal information may be exposed to hackers because of insufficient data security measures at companies. Many jurisdictions, however, do not recognize an injury suitable to judicial resolution unless and until hackers use the fruits of their hacking for nefarious purposes that directly impact the victims, such as credit card fraud or identity theft. Victims are therefore left in the position of having to decide whether to spend their time, money, and effort monitoring their credit and other accounts — knowing that they may never be able to recover — or forgoing preventive measures and leaving their financial and personal accounts vulnerable to misuse. If recent cases like *Clapper* and *Spokeo* are any indication, the U.S. Supreme Court is shifting to ever more restrictive Article III standing requirements. Consequently, it is up to Congress to pass comprehensive legislation that will afford data breach victims an adequate remedy.