Volume 65
Issue 6 *V.65, Tolle Lege*

Article 2

2-3-2021

# The District of Columbia Circuit Finds Article III Standing Based on the Risk of Future Identity Theft in In re U.S. Office of Personnel Management Data Security Breach Litigation

Briana L. Borgolini

# Note

## THE DISTRICT OF COLUMBIA CIRCUIT FINDS ARTICLE III STANDING BASED ON THE RISK OF FUTURE IDENTITY THEFT IN *IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION*

BRIANA L. BORGOLINI*

> "The Internet has brought incredible opportunity, incredible wealth. It gives us access to data and information that are enhancing our lives in all sorts of ways. It also means that more and more of our lives are being downloaded, being stored, and as a consequence are a lot more vulnerable."[1]

### I. AN INTRODUCTION TO DATA BREACH LITIGATION

The effects of identity theft can haunt data breach victims for years.[2] Some victims report the need to constantly shut down fraudulent accounts.[3] Likewise, some report countless fraudulent inquiries on their credit reports.[4] Some victims even report fraudulent tax returns filed in their names.[5] Many consumers believe there is not much they can do to protect their data in the first place.[6]

* J.D. Candidate, 2021, Villanova Charles Widger School of Law; B.A. 2014, Brown University. This Note is dedicated to my parents, Caren and Ron Borgolini, who have never stopped believing in me. I would additionally like to sincerely thank all members of the *Villanova Law Review* who provided thoughtful and invaluable feedback throughout the publication process.

1. Barack Obama, President, United States of America, Remarks by the President on the Cybersecurity National Action Plan (Feb. 17, 2016) *in* WHITE HOUSE PRESIDENT BARACK OBAMA, https://obamawhitehouse.archives.gov/the-press-office/2016/02/17/remarks-president-cybersecurity-national-action-plan [https://perma.cc/47JY-YUJ4].

2. *See* Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), https://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html [https://perma.cc/H2QM-HQYA].

3. *See* Anna Bahney, *Identity Theft Nightmares: 'I've Spent My Lifetime Building up My Credit'*, CNN MONEY (Sept. 29, 2017, 11:11 AM), https://money.cnn.com/2017/09/29/pf/identity-theft/index.html [https://perma.cc/9MNK-699X].

4. *See* Laura Shin, *'Someone Had Taken Over My Life': An Identity Theft Victim's Story*, FORBES (Nov. 18, 2014, 9:18 AM), https://www.forbes.com/sites/laurashin/2014/11/18/someone-had-taken-over-my-life-an-identity-theft-victims-story/#33fc234e25be [https://perma.cc/B5XM-NZAV].

5. *See* Hsu, *supra* note 2.

6. *See id.* (noting many consumers are not optimistic about amount of control retained over personal information).

In recent years, data breach occurrences have increased dramatically.[7] Estimates show around 2.5 billion consumers were impacted by a data breach in 2018.[8] The increasing use of technology and constantly improving skills of hackers has contributed to the prevalence of recent data breaches.[9] Additionally, data breaches can compromise a wide variety of private information.[10] The FBI's Internet Crime Complaint Center reported that cybercrime caused "$2.7 billion in financial losses in 2018."[11] This marked increase in cyberattacks resulted in more data breach litigation.[12]

One challenge victims of data breaches face when seeking legal relief is satisfying the Article III standing requirements.[13] Meeting Article III standing

---

7. Jon R. Knight, *The New Normal: Easier Data Breach Standing Is Here to Stay*, CYBERSECURITY L. REP. 1 (Feb. 6, 2019), https://www.bsfllp.com/images/content/3/4/v4/3403/2019-02-06-The-New-Normal-Easier-Data-Breach-Standing-Is-Here-to.pdf [https://perma.cc/QXZ8-JEH3] (explaining data breaches are becoming increasingly common); *see also* Aaron Holmes, *The Biggest Hacks of 2019 So Far*, BUS. INSIDER (Sept. 11, 2019), https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9 [https://perma.cc/S9XH-MUFF] (noting large numbers of unprecedented cyberattacks have occurred in only nine months of 2019); Paige Leskin, *The 21 Scariest Data Breaches of 2018*, BUS. INSIDER (Dec. 30, 2018), https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12 [https://perma.cc/67TG-BVZJ] (listing and discussing most impactful data breaches in 2018). Most of the attacks that occurred in the first nine months of 2019 appear to be financially motivated. *See* Holmes, *supra*.

8. *See* Knight, *supra* note 7 (explaining data breaches' impact on public).

9. *See* Andrew Rossow, *Why Data Breaches Are Becoming More Frequent and What You Need to Do*, FORBES (May 23, 2018, 3:12 PM), https://www.forbes.com/sites/andrewrossow/2018/05/23/why-data-breaches-are-becoming-more-frequent-and-what-you-need-to-do/#1ddb4931d97f [https://perma.cc/7ULD-TFKH] (exploring reasons for recent increases in data breaches).

10. *See id.*; *see also* Nathan Bomey, *What Does Equifax's $700M Settlement over Its Data Breach Mean for You?*, USA TODAY (July 22, 2019, 7:50 AM), https://www.usatoday.com/story/money/2019/07/22/ftc-equifax-settlement/1793029001/ [https://perma.cc/GB68-RRF2] (noting Equifax's 2017 data breach exposed wide range of personal information); Selena Larson, *Every Single Yahoo Account Was Hacked—3 Billion in All*, CNN MONEY (Oct. 4, 2017, 6:36 AM), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html [https://perma.cc/X6XN-G2DY] (detailing variety of information compromised for all Yahoo users).

11. *Report Shows Cyber-Enabled Crimes and Costs Rose in 2018*, FBI (Apr. 22, 2019), https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219 [https://perma.cc/7W65-NQ79] (explaining impact of cybercrimes in general). The FBI receives more than 900 complaints of cybercrime each day; data breaches are among the most frequently reported. *Id.*

12. *See, e.g.*, David Balser, Phyllis Sumner, Stewart Haskins & John Toro, *Insight: Data Breach Litigation Trends to Watch*, BLOOMBERG L. (Mar. 4, 2019), https://news.bloomberglaw.com/privacy-and-data-security/insight-data-breach-litigation-trends-to-watch [https://perma.cc/4JUA-5PD6] (observing data breach litigation will increase as data breaches increase); Joseph J. Lazzorotti, Jason C. Gavejian & Maya Atrakchi, *Fourth Circuit Weighs in on Standing in Data Breach Litigation*, JACKSON LEWIS (July 2, 2018), https://www.workplaceprivacyreport.com/2018/07/articles/consumer-privacy/fourth-circuit-weighs-in-on-standing-in-data-breach-litigation/ [https://perma.cc/9W9P-VGY8] (noting increases in cyber incidents have also led to increases in data breach litigation).

13. *See generally* Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 103–04 (2017) (explaining what plaintiffs must establish to show standing). Plaintiffs must show Article III standing to bring their claim in federal court. *Id.* at 82.

requirements is crucial for plaintiffs in data breach cases because many plaintiffs bring these claims as class actions, which are often brought in federal court.[14] Additionally, when plaintiffs sue in state court, the defendants often remove the action to federal court.[15] The Supreme Court's decision in *Spokeo, Inc. v. Robins*[16] has led to an increase in courts recognizing injury in data breach cases.[17] These holdings allow more victims of data breaches to meet standing requirements and bring claims against the organizations responsible for protecting their data.[18] A circuit split nevertheless exists, and some circuits refuse to recognize the risk of future identity theft as an Article III injury.[19] The split centers around whether the plaintiff can show injury simply by alleging that a breach puts them at increased risk of fraud.[20] According to the U.S. Court of Appeals for the District of Columbia's holding in *In re U.S. Office of Personnel Management Data Security Breach Litigation* (*In re OPM Litigation*),[21] circuits continue to find standing where plaintiffs merely allege an increased risk of future fraud.[22] The Supreme Court has not yet addressed this issue, leaving one's right to bring data breach claims based on the risk of future identity theft dependent upon jurisdiction.[23]

This Note argues the District of Columbia Circuit's decision in *In re OPM Litigation* is consistent with the Supreme Court's interpretation of Article III standing requirements and the Court's precedent because an increased risk of identity theft is

14. *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 690 (7th Cir. 2015) (noting plaintiffs sued as a class); *see also In re* SuperValu, Inc., 870 F.3d 763, 765 (8th Cir. 2017) (explaining that plaintiffs filed as a class). Further, the Class Action Fairness Act passed in 2005 resulted in a dramatic increase in state law class actions being litigated in federal court. *See* Jay Tidmarsh, *Finding Room for State Class Actions in a Post-CAFA World: The Case of the Counterclaim Class Action*, 35 W. ST. U. L. REV. 193, 195 (2007); *see also* Lorio, *supra* note 13, at 82 n.16 (explaining some reasons data breach cases are typically brought in federal court).

15. *See, e.g.*, Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 527 (D. Md. 2016) (noting defendants removed case to federal court); *see also* Lorio, *supra* note 13, at 82 n.16 (explaining reasons class actions are often in federal court).

16. 136 S. Ct. 1540 (2016).

17. *See* Knight, *supra* note 7 (noting courts increasingly find standing in data breach litigation when claimed injury is increased risk of future identity theft).

18. *See id.* (explaining post-*Spokeo, Inc.* impact on data breach plaintiffs).

19. *See* Luke Martin, *Resolving the Circuit Split on Article III Standing for Data Breach Suits*, COLUM. BUS. L. REV. (Aug. 13, 2019), https://journals.library.columbia.edu/index.php/CBLR/announcement/view/181 [https://perma.cc/35GE-87Z2] (explaining D.C., Third, Sixth, Seventh, Ninth, and Eleventh Circuits allow standing in cases where no misappropriation had occurred yet while Second, Fourth and Eighth Circuits do not).

20. *See* Martin, *supra* note 19 (explaining split in interpretation on whether a data breach alone may constitute injury).

21. 928 F.3d 42 (D.C. Cir. 2019).

22. *See id.* at 59 (holding plaintiffs have adequately alleged injury sufficient for standing because they have shown a risk of future identity theft). The court rejected arguments that the risk of future injury was too speculative, that the passage of time reduced certainty of future injury, and that the nature of the database being hacked made it less likely the motivation for the attack was financial gain. *See id.* at 56, 59.

23. *See* Alison Frankel, *D.C. Judge: No Actual Damages, No Claims for Data Breach Victims*, REUTERS (Feb. 4, 2019, 3:05 PM), https://www.reuters.com/article/legal-us-otc-data-breach/dc-judge-no-actual-damages-no-claims-for-data-breach-victims-idUSKCN1PT23W [https://perma.cc/D22C-7KQB] (noting only some circuits allow plaintiffs to sue when information has been compromised).

a sufficient injury to confer standing.[24] Finding standing in cases involving data breaches is necessary to hold companies accountable for their role in data breaches.[25] Further, a statutory solution will not be sufficient to remedy data breach plaintiffs' barrier to courts.[26] Part II discusses Article III standing and the current circuit split over in data breach cases. Part III sets forth the facts of *In re OPM Litigation*. Part IV explains the reasoning for the District of Columbia Circuit's decision. Part V argues that it is consistent with Supreme Court precedent, that such a holding is necessary to incentivize companies to improve practices, and that a statutory solution will not be enough to confer standing. Finally, Part VI explores this decision's impact on data breach litigation.

## II. THE BACKGROUND OF DATA BREACH LITIGATION

Data breaches occur at a high rate in part because of the frequent use of electronic storage methods to maintain data.[27] In 2018 alone, data breaches impacted billions of people.[28] Unsurprisingly, the number of lawsuits brought by victims of such breaches is also increasing, leading to constant development in data breach litigation.[29] Data breach litigation, however, is often restricted by the Article III standing doctrine.[30] The Supreme Court has not yet resolved the inconsistency among circuits.[31]

---

24. For further discussion of Supreme Court precedent and data breach standing, see *infra* Section V.A.

25. *See* Clara Kim, Note, *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, 575-76, 581 (explaining how increased recognition of standing in data breach cases will hold companies accountable).

26. *See* Megan Dowty, Note, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 697, 700 (2017) (noting injury will often still be required when there is violation of statute).

27. *See* Andrew Braunstein, Note, *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, 103 (2016) (noting continued movement towards electronic storage is one reason for increasing occurrence of data breaches).

28. *See* Mike Snider, *Your Data Was Probably Stolen in a Cyberattack in 2018—and You Should Care*, USA TODAY (Dec. 28, 2018), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/ [https://perma.cc/YX58-Z4VB].

29. *See* Miles L. Galbraith, Comment, *Identity Crisis: Seeking A Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U.L. REV. 1365, 1374 (2013) (explaining data breach litigation is rapidly developing). For further discussion of background on data breaches and litigation, see *infra* Section II.A.

30. *See* Nicholas Green, Note, *Standing in the Future: The Case for a Substantial Risk Theory of "Injury in Fact" in Consumer Data Breach Class Actions*, 58 B.C. L. REV. 287, 288 (2017) (noting injury in fact element of standing makes it difficult for plaintiffs to bring claims). For further discussion of standing doctrine, see *infra* Section II.B.

31. *See* Frankel, *supra* note 23 (noting Supreme Court has yet to examine issue of standing in data breach cases); *see also* Lorio, *supra* note 13, at 91–101 (explaining circuit court standing outcomes in data breach litigation). For further discussion of the Supreme Court's interpretations of the standing doctrine, see *infra* Section II.C (discussing recent Supreme Court standing decisions informing analysis in data breach cases). For further discussion of the current circuit split, see *infra* Section II.D (discussing current circuit split regarding when data breach plaintiffs have shown sufficient injury for Article III standing).

### A. *The Impact of Data Breaches*

Data breaches have become common because of the increase in electronic information storage.[32] Hackers have an easier time accessing electronically stored information, increasing the risk consumers face.[33] Estimates show that data breaches impact a high percentage of major organizations.[34]

The type of information stolen typically informs the nature of the harm to the consumer.[35] Harms may range from needing to cancel a credit card to having one's credit history ruined.[36] These variable harms are often what victims bring to litigation.[37] Regardless of the precise harm, consumers primarily feel the negative effects of poor data management practices.[38]

The lack of federal laws governing the duties of organizations that store sensitive data makes obtaining a legal remedy difficult.[39] Rather than being guided by a comprehensive framework, liability in data breaches is covered by a "patchwork of laws" that often address specific issues and not data breach litigation as a whole.[40] Under state and federal laws, liability is not imposed automatically when a breach

32. *See* Braunstein, *supra* note 27, at 103–04 (noting increase in electronic storage of information); Galbraith, *supra* note 29, at 1373–74 (explaining issues raised by data breach litigation are modern, as a result of the increase in technology use); *see also* Daniel Funke, *By the Numbers: How Common Are Data Breaches—and What Can You Do About Them?*, POLITIFACT (Sept. 23, 2019, 9:46 AM), https://www.politifact.com/truth-o-meter/article/2019/sep/23/numbers-how-common-are-data-breaches-and-what-can-/ [https://perma.cc/5NXC-45EG] (noting increasingly common occurrence of data breaches since 2005).

33. *See* Braunstein, *supra* note 27, at 104 (noting impact increased technology has on consumers and susceptibility to being victims of data breaches).

34. Aaron Wynhausen, Note, *The Eight Circuit Further Complicates Plaintiff Standing in Data Breach Cases*, 84 MO. L. REV. 297, 298 (2019) (citing Galbraith, *supra* note 29, at 1368) (noting frequency at which large companies are impacted by data breaches or cyberattacks).

35. *See* Green, *supra* note 30, at 290 (explaining impact and possible injuries that data breaches can have on consumers); *see also* Wynhausen, *supra* note 34 at 297.

36. *See* Green, *supra* note 30, at 290.

37. *See id.*

38. *See* Braunstein, *supra* note 27, at 105 (explaining how "consumers bear the brunt of the harm" when a data breach occurs).

39. *See* Wynhausen, *supra* note 34, at 298 (explaining current difficulties plaintiffs face in seeking legal recourse after their information has been compromised); *see also* Kim, *supra* note 25, at 550 (noting lack of appropriate legal recourse in response to increasing occurrence of data breaches).

40. *See* Kim, *supra* note 25, at 554 (explaining current state of data breach regulatory scheme is not comprehensive and is more confusing than helpful). State and federal agencies make these laws, which vary in what they address. *See id.* at 551. Further, many federal legal schemes in place are not effective at serving affected consumers because they address narrow issues within specific industries. *See id.* at 554.

occurs.[41] Rather, plaintiffs must satisfy certain requirements for the organization to be held liable.[42]

### B. *The Interpretation of Article III Standing Requirements*

The Constitution states that only "cases" and "controversies" may be heard in federal court.[43] However, the Supreme Court has interpreted the "cases" and "controversies" language to mean that only plaintiffs who have standing may be heard in federal court.[44] Article III therefore restricts federal court jurisdiction to "cases" and "controversies."[45] To satisfy Article III standing, the Supreme Court requires plaintiffs to show they suffered an injury.[46] Federal courts must dismiss the case and cannot consider the merits of a plaintiff's claim where there is no injury sufficient for standing.[47]

The standing requirement is grounded in the constitutional principles that advisory opinions are forbidden and the federal courts should not exceed their constitutional limits.[48] Besides limiting the role of federal courts, the standing requirement serves other purposes.[49] First, the doctrine guarantees that a decision will primarily impact plaintiffs, therefore preventing claims that may be brought by "concerned bystanders."[50] In addition, the doctrine minimizes the litigation of "abstract injuries

41. *Who Is Liable When a Data Breach Occurs?*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability [https://perma.cc/8LLQ-SK7N] (last visited Sept. 12, 2019) (explaining when a company or organization may be held liable for a data breach under current legal framework); *see also* Usama Kahf, *Is There Automatic Civil Liability for a Data Breach?*, FISHER PHILLIPS (Nov. 14, 2017), https://www.fisherphillips.com/Employment-Privacy-Blog/is-there-automatic-civil-liability-for-data-breach [https://perma.cc/JL72-F3RR] (describing instances where a company or organization may be liable for data breach harms and explaining liability is not automatic).

42. *See Who Is Liable When a Data Breach Occurs?*, *supra* note 41 (explaining specific requirements that must be found before liability may be imposed).

43. *See* Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1328–29 (2017) (explaining how Supreme Court came to require standing for plaintiffs bringing suit in federal court); *see also* Galbraith, *supra* note 29, at 1375 (noting Supreme Court has inferred standing requirements from text of Constitution).

44. *See* Mank, *supra* note 43, at 1328–29 (detailing Article III's limitation on judiciary).

45. *See* Lorio, *supra* note 13, at 83 (discussing justiciability requirements and explaining certain requirements must be met before one can bring claim in federal court).

46. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992). Article III standing requirements ensure the judiciary hears only cases that fall within its constitutional authority. *See id.* at 560.

47. *See* Galbraith, *supra* note 29, at 1376 (explaining restrictions imposed on federal courts regarding which cases they may hear).

48. *See* Mank, *supra* note 43, at 1329 (explaining requirement of Article III standing and noting why requirement is important). The article also notes that it is important to ensure federal courts have a "properly limited [] role" in a democracy. *Id.* (quoting Daimler Chrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (explaining the limited role of federal courts)).

49. *See* Galbraith, *supra* note 29, at 1386 (noting recent standing doctrine application to data breach claims fails to further justiciability principles).

50. *See id.* at 1385–86 (quoting U.S. v. Students Challenging Reg. Agency Procedures (SCRAP), 412 U.S. 669, 687 (1973)). "[T]he Court has said: '[t]he exercise of judicial power, which can so profoundly affect the lives, liberty, and property of those to whom it extends, is therefore restricted to litigants who can show "injury in fact" resulting from the action which they seek to have the court adjudicate.'" *Id.* (quoting Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 473 (1982).

such as violations of generalized rights . . . ."[51] Injury in fact is the element of standing most often at issue in data breach cases.[52]

Plaintiffs in data breach cases often struggle to show Article III standing requirements under Supreme Court jurisprudence.[53] To satisfy Article III standing, plaintiffs must allege an injury that is "concrete and particularized[,] and . . . actual and imminent."[54] In data breach cases, plaintiffs often struggle to show injury—especially when their information has yet to be misappropriated.[55] The Supreme Court has not decided the issue of Article III standing in data breach cases, but it has analyzed other future injuries that are applicable to data breach litigation.[56]

First, the Court has recognized that future injuries must be "actual or imminent" to satisfy the injury requirement for standing.[57] In 2013, the Supreme Court decided *Clapper v. Amnesty Int'l USA*[58] and held an "objectively reasonable likelihood" of future injury could not meet the elements of standing.[59] In *Clapper*, the plaintiffs asserted two theories of injury, mirroring the arguments often made by plaintiffs in data breach cases.[60] In rejecting the plaintiffs' theories, the Court reasoned that any risk of future injury must be "certainly impending" to be sufficient

51. *Id.* at 1386. The Supreme Court will not hear cases concerning "the generalized interest of all citizens." *Id.* (internal quotation marks omitted) (quoting *Valley Forge*, 454 U.S. at 483).

52. *See* Lorio, *supra* note 13, at 84 (explaining injury is standing element that is difficult for data breach litigants to prove); *see also* Wynhausen, *supra* note 34, at 305 (noting standing is typically "major hurdle" plaintiffs must conquer).

53. *See* Lorio, *supra* note 13, at 81–82 (noting many courts will not find standing in data breach cases); Kim, *supra* note 25, at 557 (noting data breach plaintiffs often cannot sufficiently allege standing).

54. Priscilla Fasoro & Lauren Wiseman, *Standing Issues in Data Breach Litigation: An Overview*, INSIDE PRIVACY (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/ [https://perma.cc/8E5J-2VLK].

55. *See* Fasoro & Wiseman, *supra* note 54 (noting in data breach cases, standing elements are often harder to meet given unique injuries at issue).

56. *See* Section II.C (discussing Supreme Court precedent relating to data breach cases).

57. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)); *see also* Lorio, *supra* note 13, at 84-86 (detailing *Clapper*'s impact on "actual or imminent" element of Article III injury).

58. 568 U.S. 398 (2013).

59. *See id.* at 410, 416 (finding risk of future harm is hypothetical and plaintiffs cannot create an injury by spending money seeking to avoid hypothetical future harm). The Court noted such a claim "improperly waters down the fundamental requirements of Article III." *Id.* at 416.

60. *See id.* at 407 (explaining arguments set forth by plaintiffs in support of satisfaction of Article III standing elements). First, they alleged an "objectively reasonable likelihood" that injury would occur based on a likelihood that improper surveillance will eventually intercept their data. *Id.* Next, they alleged that they incurred costs to prevent or reduce their risk of future injury. *Id.* Plaintiffs in *Clapper* alleged a risk of future harm when they argued they would need to "take costly and burdensome measures" to mitigate risks. *See id.* at 402. In data breach cases, plaintiffs often allege risk of future injuries and a need to mitigate risks imposed on them by the data breach. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386–87 (6th Cir. 2016) (noting plaintiffs argue future risk of identity theft and expenses incurred to reduce future risk); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1211, 1216 (N.D. Cal. 2014) (explaining plaintiffs alleged both an increased risk of future misappropriation and reasonable costs to mitigate risk).

for injury in fact.[61] Practitioners and courts view this holding as inhibiting plaintiffs' ability to meet standing requirements.[62]

Later, the Court held in *Spokeo, Inc. v. Robins*[63] that a risk of future injury may satisfy the "concreteness" requirement of standing.[64] Similar to the injury raised in many data breach cases, the plaintiff in Spokeo alleged they suffered an intangible injury as opposed to tangible.[65] In assessing whether the injury was sufficiently concrete, the Court noted that the injury must be "real" rather than "abstract," and intangible harm must be considered in light of "both history and the judgment of Congress."[66] The Court also noted that a procedural violation of a statute alone is insufficient to show concrete injury.[67] In discussing the risk of future injury, the Court recognized the risk of real harm can sometimes satisfy the concreteness requirement where the plaintiff can allege that Congress intended to remedy their particular harm.[68] Despite these recent holdings, circuit courts remain split on the issue facing data breach plaintiffs, leaving victims with inconsistent remedies across circuits.[69]

### C. *Circuit Courts' Examination of Article III Standing in Data Breach Cases*

The circuit courts remain split over whether the increased risk of future identity theft is sufficient to show injury required for standing.[70] While a number of courts have allowed such cases to proceed, some still refuse to expand the scope of Article

61. *See Clapper*, 568 U.S. at 422 (holding plaintiffs' speculative allegations and standing theory not sufficient to show injury).

62. *See* Claire Wilka, Note, *The Effects of* Clapper v. Amnesty International USA*: An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGHTON L. REV. 467, 470–71 (2016) (explaining *Clapper*'s effect on plaintiffs' ability to bring claims); *see also* Arthur R. Vorbrodt, Note, Clapper *Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison*, 73 WASH. & LEE L. REV. ONLINE 61, 87 (2016) (noting *Clapper* has been interpreted to restrict who may establish Article III standing, and many courts have viewed this as raising bar in data breach cases specifically).

63. 136 S. Ct. 1540 (2016).

64. *See id.* at 1548–49 (discussing requirement that injury must be concrete to satisfy Article III standing elements); *see also* Lorio, *supra* note 13, at 87–89 (explaining how Supreme Court treated concreteness requirement of standing in *Spokeo, Inc.*).

65. *See Spokeo, Inc.*, 136 S. Ct. at 1546, 1549. Plaintiff alleged that at some time, an individual searched for plaintiff and found false information in the database run by Spokeo, Inc. *See id.* at 1546. This is considered an intangible injury as opposed to tangible because it is not an injury like losing a job or income. *See* Lorio, *supra* note 13, at 88–89 (noting examples of tangible injury).

66. *Spokeo, Inc.*, 136 S. Ct. at 1548–49 (explaining what Court will consider when deciding whether claimed injury is sufficiently concrete). Further, the Court noted that the "case-or-controversy" requirement of the Constitution gave rise to the standing doctrine, and tradition should inform the inquiry of whether harm occurred. *Id.* at 1549. Finally, the Court explained that Congress is "well positioned to identify intangible harms." *Id.*

67. *See id.* at 1549.

68. *See id.* (explaining what types of injuries may satisfy the concreteness requirement). The Court noted there may be circumstances where a plaintiff can sufficiently show concrete injury by alleging a violation of a procedural right. *See id.*

69. *See infra* Section II.C (discussing circuit split and explaining various outcomes related to standing in data breach claims).

70. *See* Martin, *supra* note 19 (explaining current circuit split regarding standing in data breach cases); *see also* Frankel, *supra* note 23 (noting current circuit split and impact on data breach litigation).

III standing to allow them to be heard.[71] While the D.C., Sixth, Seventh, and Ninth circuits have allowed these claims to move forward with an alleged risk of future injury, the Second, Third, Fourth, and Eighth circuits have not.[72] A number of circuit courts have found standing where plaintiffs allege an increased risk of identity theft. In *Attias v. CareFirst, Inc.*,[73] the court held the plaintiff established injury because information had already been compromised and there was no longer a hypothetical risk of injury.[74] In *Krottner v. Starbucks Corp.*,[75] the Ninth Circuit found that stolen, unencrypted person information stored on a laptop created an increased risk of identity theft.[76] The court asserted that this risk was credible.[77]

Similarly, in *Lewert v. P.F. Chang's China Bistro, Inc.*,[78] the Seventh Circuit found that, where customer financial information was compromised and consumers were at risk for future identity theft (and in fact, one did experience instances of fraudulent activity), injury requirements were met.[79] The Seventh Circuit applied similar reasoning in *Remijas v. Neiman Marcus Group, LLC*,[80] finding that plaintiffs showed sufficiently substantial risk of future harm to satisfy standing when customer

71. *See* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (refusing to recognize injury for an increased risk of identity theft); *see also* Lorio, *supra* note 13, at 91–101 (assessing circuit court's various outcomes on standing and noting some do not recognize risk of future theft as injury).

72. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017) (finding injury where victims alleged hackers obtained all information necessary to steal the victim's identity); *Beck*, 848 F.3d at 274 (holding requirements for standing were not met when plaintiffs could not show that information was misused); *In re* SuperValu, Inc., 870 F.3d 763, 770–72 (8th Cir. 2017) (declining to find injury where information was stolen but not misused); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (holding plaintiff did not show standing where their card was not charged and they did not show expenditures to prevent theft); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 389 (6th Cir. 2016) (finding plaintiffs alleged standing where data was clearly in hands of nefarious criminals); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (holding plaintiffs showed standing where financial information was compromised); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (finding plaintiffs had standing when private information was stolen from a customer database); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding any future injury was speculative and therefore insufficient for Article III standing); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that when someone stole a computer containing sensitive information, plaintiff suffered real and increased risk of identity theft); *see also* Lorio, *supra* note 13, at 91–101 (detailing various circuit court outcomes in data breach standing analyses).

73. 865 F.3d 620 (D.C. Cir. 2017).

74. *See id.* at 628–29 (explaining why court in *Attias* found future harm was not uncertain). In reaching its holding, the court found it important that all information necessary for identity theft was compromised. *See id.*

75. 628 F.3d 1139 (9th Cir. 2010).

76. *See id.* at 1143 (finding plaintiffs "alleged a credible threat of real and immediate harm" when they alleged stolen laptops contained sensitive information).

77. *See id.* (explaining holding of Ninth Circuit). The court contrasted the risk of future fraud due to misuse of data on a stolen computer against a hypothetical risk of stealing the computer in the first place. *See id.* The court noted that the latter would be too speculative for standing because the risk of identity fraud based on the computer's potential to be stolen would be too far removed. *See id.*

78. 819 F.3d 963 (7th Cir. 2016).

79. *See id.* at 967 (holding circumstances of case showed sufficiently imminent injury in fact to satisfy standing requirements). Plaintiffs here also spent time and money in an effort to mitigate the effects of the breach through credit monitoring. *See id.*

80. 794 F.3d 688 (7th Cir. 2015).

information was compromised due to a database breach.[81] In *Remijas*, the court also noted that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing."[82] Further, in *Galaria v. Nationwide Mutual Insurance Company*,[83] the Sixth Circuit found standing where private personal and financial information was intentionally stolen and plaintiffs showed it would likely be used for fraudulent purposes.[84]

In contrast, some circuits do not recognize such injuries as sufficient to constitute standing.[85] In *Beck v. McDonald*,[86] the Fourth Circuit held that there was no injury where plaintiffs could not show that information contained on a stolen laptop was misused, or that the thief intended to misuse the information.[87] Likewise, in *Reilly v. Ceridian Corp.*,[88] the Third Circuit found that where allegations of a future injury required speculation, injury was not sufficiently imminent for the purposes of standing.[89]

Moreover, the Eight Circuit in *In re SuperValu, Inc.*[90] declined to recognize injury where plaintiffs' information was compromised but no misuse occurred.[91] Similarly, the Second Circuit refused to find injury in *Whalen v. Michaels Stores, Inc.*[92] when plaintiff could not show they incurred losses, even where attempted identity theft occurred.[93] As a result, the holdings of district courts are similarly split, leaving plaintiffs' abilities to bring their claims dependent on where they are located.[94]

---

81. *See id.* at 693 (finding plaintiffs showed substantial enough risk of future harm to satisfy standing). Further, the court emphasized that certain inferences could be drawn in situations such as the one at hand, asking the question: "Why else would hackers break into a . . . database and steal customers' private information? Presumably, the purpose of the hack is . . . to make fraudulent charges or assume those consumers' identities." *Id.*

82. *Id.*

83. 663 Fed. App'x 384 (6th Cir. 2016).

84. *See id.* at 389 (noting where reasonable inference of malicious intent could be drawn, future injury could satisfy requirements of standing).

85. *See* Lorio, *supra* note 13, at 91–101 (assessing circuit court's various outcomes on standing and noting some do not recognize risk of future theft as injury).

86. 848 F.3d 262 (4th Cir. 2017).

87. *See id.* at 274 (finding plaintiffs did not allege sufficient injury when they could not show information was misused or at any risk of being misused).

88. 664 F.3d 38 (3d Cir. 2011).

89. *See id.* at 42 (holding alleged injuries were too remote for Article III standing).

90. 870 F.3d 763 (8th Cir. 2017).

91. *See id.* at 770–72 (explaining plaintiffs' allegations of increased risk of future identity theft cannot satisfy standing). The court noted that while some card information was stolen, identity theft was not a substantial risk because social security numbers were not stolen. *See id.* at 770. In contrast, the court did recognize injury for one plaintiff who could show he experienced actual identity theft. *See id.* at 773.

92. 689 F. App'x 89 (2d Cir. 2017).

93. *See id.* at 90 (noting agreement with district court that plaintiff had not shown charges to their card, or expenditures monitoring her credit that could constitute injury).

94. *See, e.g.*, Oneal v. First Tenn. Bank, No. 4:17-CV-3-TAV-SKL, 2018 WL 1352519, at *1 (E.D. Tenn. Mar. 15, 2018) (noting injury is not sufficiently concrete for standing where alleged injury is an unathorized credit inquiry that could lead to future harm); Fero v. Excellus Health Plan Inc., 304 F. Supp. 3d 333, 345 (W.D.N.Y. 2018) (holding future harm of identity theft was sufficient when circumstances suggested hackers likely intended to misappropriate information); Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 532 (D. Md. 2016) (finding plaintiffs sufficiently allege injury where instances of theft occurred, or where they can show purpose of breach was

## III. THE FACTS OF *IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION*

The District of Columbia Circuit examined the standing issue in data breach cases in *In re OPM Litigation*.[95] The U.S. Office of Personnel Management (OPM) is the main human resource agency of the federal government.[96] The OPM electronically stores personal information on federal employees as well as millions of individuals who submitted to federal background checks.[97] In 2014, OPM experienced multiple cyberattacks that compromised the private information of nearly 21.5 million people.[98] The stolen information from the breach included "current and prospective employees' Social Security numbers, birth dates, and residency details, along with approximately 5.6 million sets of fingerprints."[99] The breach also compromised personal information about employees' relatives.[100]

Affected individuals have since experienced varying types of financial fraud, and many as-of-yet unaffected individuals fear future identity theft.[101] OPM offered some individuals free fraud monitoring, identity theft protection, and insurance for a period of time.[102] Many people filed lawsuits against OPM and Keypoint, an investigation and security partner that handled many background checks for the federal government, after these measures did not rectify their fears.[103]

Some plaintiffs alleged OPM had notice that its systems were "prime targets" for cyberattacks, and that KeyPoint failed to meet industry standards in maintaining OPM's information security defenses.[104] Plaintiffs further alleged hackers

---

identity theft); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding plaintiffs had alleged actual injury because a number of consumers experienced instances of identity fraud such as unauthorized charges, compromised bank accounts, and other financial losses); *see also* Lorio, *supra* note 13, at 102–03 (providing examples of district court outcomes in data breach standing cases).

95. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig. (*In re OPM Litig.*), 928 F.3d 42, 49, 53 (D.C. Cir. 2019) (noting plaintiffs were exposed to a heightened risk of identity theft and district court improperly dismissed claim for lack of Article III standing); *see also* Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017) (examining whether plaintiffs had standing after data breach).

96. *See In re OPM Litig.*, 928 F.3d at 49 (explaining role of OPM).

97. *See id.* (illustrating scope of data possessed by OPM).

98. *See id.* at 50 (explaining OPM experienced multiple cyberattacks between November 2013 and November 2014). Some of these attacks went unnoticed for months. *Id.*

99. *See id.* (showing range of information compromised by cyberattacks).

100. *See id.* (explaining how data breaches impacted more than just federal employees).

101. *See id.* (explaining cyberattack's impact on those affected).

102. *See id.* (describing steps OPM took to assist individuals impacted by breach).

103. *See id.* (explaining plaintiffs sued because offered services failed to alleviate affected parties' concerns). The Court split the suits into two complaints. *Id.* First, thirty-eight victims of the breach, along with a putative class, sued OPM. *Id.* Second, the National Treasury Employees Union sued for declaratory and injunctive relief. *Id.* This Note will focus on the first complaint.

104. *See id.* at 51 (explaining basis for plaintiffs' claim). Plaintiffs asserted OPM experienced similar data breaches in the past and that their network experienced a "large number of hacking attempts." *Id.* Plaintiffs alleged that OPM's Inspector General reported weaknesses in OPM's network protections. *See id.* Plaintiffs further alleged that "KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' [personal information] and the credentials used to access it . . . ." *Id.* (alteration in original) (quoting Consolidated Amended Complaint at J.A. 98, *In re OPM Litig.*, 928 F.3d at 51 (No. 1:15-mc-01394)).

specifically targeted personal information for theft, noting that some plaintiffs had already experienced malicious use of their personal information.[105] OPM and KeyPoint moved to dismiss the claims on Article III standing grounds.[106] The district court declined to recognize an increased risk of future identity theft as sufficient to show standing and granted defendants' motion to dismiss.[107] On appeal, the District of Columbia Circuit held that the plaintiffs had sufficiently alleged injury in fact as required for Article III standing.[108]

## IV. A NARRATIVE ANALYSIS OF *IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION*

In *In re OPM Litigation*, the D.C. Circuit assessed whether plaintiffs whose personal information was compromised but not yet used fraudulently had sufficient injury for Article III standing.[109] While plaintiffs alleged numerous harms, the court focused on their increased risk of future identity theft, as all plaintiffs alleged that harm.[110] The court began by identifying recent Supreme Court standing precedent.[111] It then examined the plaintiffs' claims in light of its prior holding in *Attias*, where it found that plaintiffs' substantial risk of future identity theft satisfied standing.[112] Finally, the court rejected OPM's argument that government breaches are motivated by interests other than fraud and distinguished the present case's facts from those OPM cited.[113]

### A. *The Court Assesses Supreme Court and Circuit Precedent*

The D.C. Circuit examined recent Supreme Court holdings to support its conclusion that plaintiffs' increased risk of future identity theft satisfies Article III standing's injury requirement.[114] The court first noted that in *Spokeo, Inc.*, the Supreme Court held that injury must be "concrete and particularized and actual or imminent,

105. *See id.* at 52, 58 (explaining plaintiffs alleged attacks targeted their information for improper use). Plaintiffs alleged attackers misused their information through "improper use of their Social Security numbers, unauthorized charges to existing credit card and bank accounts, fraudulent openings of new credit card and other financial accounts, and the filing of fraudulent tax returns . . . ." *Id.* at 52.

106. *Id.* at 53.

107. *Id.* (noting district court granted OPM and KeyPoint's motions to dismiss for lack of standing).

108. *Id.* (reconsidering whether plaintiffs alleged sufficient injury in fact for standing).

109. *See id.* (explaining District of Columbia Circuit reversed district court on Article III standing issue). The circuit court held that "plaintiffs have alleged facts sufficient to satisfy Article III standing requirements." *Id.*

110. *See id.* at 55 (explaining court focuses on risk of future identity theft as injury when conducting standing analysis).

111. *See id.* at 54 (explaining current Supreme Court standards for injury in Article III standing). For a further discussion of the court's interpretation of Supreme Court standing precedent, see *infra* Section IV.A.

112. *See id.* at 55–56 (comparing the current case's facts to *Attias* holding). For a further discussion of the court's analysis of *Attias*, see *infra* Section IV.A.

113. *See id.* at 56–58 (discussing and rejecting arguments made by OPM). For a further discussion of the court's analysis of OPM's arguments, see *infra* Section IV.B.

114. *See id.* at 54–55 (explaining how Supreme Court standards for Article III standing apply to present case).

not conjectural or hypothetical."[115] The court also pointed out that the Supreme Court had previously held claims of future injury must be "certainly impending" or indicate a "substantial risk" of an injury occurring.[116] The court next examined the plaintiffs' argument that the district court's opinion was contrary to the circuit's holding in *Attias*.[117] It found that although the attacks were distinguishable from those in *Attias* in some ways, the OPM hackers still possessed all the information they needed for fraud like the hackers in *Attias*.[118] Further, some plaintiffs in the present case had already experienced misappropriation, which illustrated the malicious intent of the hackers.[119] The court found that these facts were similar to those in *Attias* and sufficiently showed that the plaintiffs' risk of future identity theft was substantial, rather than "merely speculative or theoretical."[120]

### B. *The Court Rejects OPM's Arguments of Hacker Motivation and Distinguishes Prior Caselaw*

The court next examined OPM's arguments: (1) unique hacker motivation for government systems cases, and (2) plaintiffs' lack of standing.[121] The D.C. Circuit ultimately rejected both theories.[122] The court first rejected the arguments that the factors motivating hackers to breach a government system are different than those motivating hackers to breach other systems, noting that while there may be other motives for one to hack a government system, it is equally possible that the purpose is to steal identities.[123] The court emphasized that the possibility of other motives does not negate the opportunity for identity theft.[124]

Next, the court found that OPM's cited cases, which held that the plaintiffs did not have injury sufficient for standing when they alleged a future risk of identity theft, were distinguishable from the present case.[125] First, the court distinguished *Beck*, where stealing a laptop containing personal information compromised data because there was no evidence of misuse or intent to misuse the data, and the risk

115. *Id.* at 54 (internal quotation marks omitted) (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016)) (noting standard for injury in fact set forth by Supreme Court in *Spokeo, Inc.*).

116. *Id.* (internal quotation marks omitted) (quoting Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014)) (noting Supreme Court's rule regarding future injury in standing cases).

117. *See id.* at 55–56 (citing Attias v. CareFirst, Inc., 865 F.3d 620, 622, 628–29 (D.C. Cir. 2017) (examining circuit court's prior opinion in *Attias* and applying to present case).

118. *See id.* at 56 (comparing OPM and Attias attacks and determining that, in either case, attackers possess information to commit identity theft). Further, the court noted that "[i]t hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft." *Id.*

119. *See id.* (explaining facts further allowed circuit court to conclude risk of future identity theft is substantial). "[H]ackers stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information." *Id.*

120. *See id.* (explaining plaintiffs in present case have alleged sufficient facts to show injury necessary for standing).

121. *See id.* at 56–59.

122. *See id.* at 56–59 (discussing and rejecting arguments made by defendant OPM).

123. *See id.* at 57 (explaining why circuit court finds OPM's argument regarding motive and intent unpersuasive). The court disagreed with the dissent's stance that other motives are more plausible in the case of an attack on a government database. *See id.*

124. *See id.* (explaining why OPM's ulterior motive argument fails).

125. *See id.* at 58 (finding facts of present case "differ markedly" from cases OPM cited).

of future harm remained speculative.[126] Similarly, the court distinguished *Reilly*, where a hacker "potentially" accessed "personal and financial information" but future harm was speculative because plaintiffs showed no evidence of misuse.[127] In contrast to *Beck* and *Reilly*, the court noted that plaintiffs in this case alleged that hackers targeted their personal information specifically for identity fraud purposes, and used it for that purpose in some cases.[128] Therefore, the substantial risk of future identity theft sufficed to show injury.[129]

## V. A CRITICAL ANALYSIS OF *IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION*

Data breach victims should have injury sufficient for standing where they can allege an increased risk of future identity theft when their information is compromised. The increased risk of future identity theft is not speculative, is sufficiently concrete under Supreme Court jurisprudence, and finding standing allows entities to be held accountable for their role in data breaches, thereby incentivizing better protection.[130] Further, a statutory solution or private right of action likely will not allow data breach plaintiffs to pursue the merits of their claims or a remedy because they would still need to show injury sufficient for Article III standing.[131]

### A. *An Increased Risk of Future Identity Theft is Concrete Injury under Supreme Court Precedent*

Satisfying the standing elements, including injury, should be a "low threshold" and should not keep data breach victims out of court.[132] Even if a narrow approach is taken following *Clapper* and *Spokeo, Inc.*, allegations of a future risk of identity theft

126. *See id.* at 58–59 (citing Beck v. McDonald, 848 F.3d 262, 274-75 (4th Cir. 2017)) (distinguishing allegations in present case from those in *Beck*).

127. *See id.* (internal quotation marks omitted) (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011)) (noting *Reilly* plaintiffs failed to establish concrete facts showing data was used for fraudulent purposes). In *Reilly*, it was "not known whether the hacker read, copied, or understood the data," and no plaintiff alleged any misappropriation. *Id.* (internal quotation marks omitted) (quoting *Reilly*, 664 F.3d at 44).

128. *See id.* at 58–59 (explaining facts of current case differ from those cited by OPM). These allegations serve to move the risk in this case from speculative to substantial. *See id.* at 59.

129. *See id.* at 59 (finding plaintiffs in case alleged facts that support possibility of a substantial risk of future identity theft).

130. *See* Kim, *supra* note 25, at 581 (explaining how companies will be pressured to improve their practices when courts may examine the merits of victims' claims); Martin, *supra* note 19 (noting that "[a]llowing plaintiffs to take advantage of the more relaxed standing requirements in those courts has the potential effect of pushing companies to invest in more comprehensive cybersecurity as a way to better protect against litigation risk and therefore better protect these consumers in the first place.").

131. *See* Dowty, *supra* note 26, at 697, 700 (2017)) (noting courts still require injury along with statutory violation). For a further discussion of future risk of identity theft as sufficient for Article III standing purposes, see *infra* Section V.A.

132. *See* Galbraith, *supra* note 29, at 1371 (explaining bar for establishing Article III standing should, in theory, be fairly low). This article also explains that successful injunctive relief may signify a cognizable injury. *See id.*

warrant a finding that the elements have been properly established.[133] In cases where plaintiffs can allege a high risk of future identify theft, such as *In re OPM Litigation*, an attenuated chain of future events does not exist and therefore does not raise the issues the Supreme Court was concerned with in *Clapper*.[134]

Plaintiffs in data breach cases may allege injury sufficient for standing based on their "substantial risk of future identity theft" and associated expenses necessary to reduce their risk.[135] This finding is compatible with *Clapper* because many plaintiffs will have already experienced attempted or actual fraudulent activity, which gives rise to the inference that victims who have not been impacted yet are likely to be in the future.[136] Importantly, this inference eliminates the possibility that a hypothetical chain of future events is required for injury to occur.[137]

Further, plaintiffs in data breach cases can at times raise "concrete" injuries such as those the Court was concerned with in *Spokeo, Inc*., where plaintiffs raised instances of attempted fraud and losses of large amounts of financial information.[138] Data breach victims may raise a "*risk* of real harm" by alleging that they are at an increased risk to have their data stolen in the future.[139] Although risk of harm is an "intangible" injury, the Court in *Spokeo, Inc.* specified that, when it held an injury

133. For a further discussion of the alignment between the D.C. Circuit's analysis and the Supreme Court's interpretation of Article III standing elements, see *infra* notes 135–42 and accompanying text.

134. *Compare In re OPM Litig.*, 928 F.3d at 59, 61 (finding standing where plaintiffs alleged an increased risk of future identity theft and spending on services to reduce risk of identity theft), *with* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013) (finding no standing where plaintiffs allege risk of future injury because chain of inferences leading to injury was too speculative and depended on many unknown events).

135. *See In re OPM Litig.*, 928 F.3d at 59 (explaining expenses plaintiffs "reasonably incurred" to protect themselves is an injury because plaintiffs succeed in alleging a risk of future identity theft). The court noted that "[t]he [Supreme] Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists." *Id.* (second alteration in original) (quoting Hutton v. National Bd. of Examiners in Optometry, Inc., 892 F.3d 613, 622 (4th Cir. 2018)); *see also Clapper*, 568 U.S. at 414 n.5 (outlining standard for Article III standing requirements if plaintiffs choose to mitigate potential harm).

136. *See In re OPM Litig.*, 928 F.3d at 56 (explaining because some information has already been used fraudulently, it can be inferred that others are at increased risk).

137. *See id.* (noting some plaintiffs have already alleged incidents of fraudulent activity as a result of information being compromised). The circuit court inferred from these facts that the risk of future identity theft is no longer speculative, but is substantial. *See id.* This substantial risk is distinguishable from *Clapper* because the *Clapper* plaintiffs showed only hypothetical harm and no inference of future injury existed. *See Clapper*, 568 U.S. at 410 (finding no injury where plaintiffs allege risk of future injury because chain of inferences leading to injury was too speculative and depended on many unknown events).

138. *See In re OPM Litig.*, 928 F.3d at 56 (explaining nature and extent of information compromised, which makes it substantially likely plaintiffs would be harmed in future); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1546 (2016) (describing facts of case and noting injury needs to come from risk of real harm besides procedural violation); Lorio, *supra* note 13, at 88 (noting plaintiff's allegation that incorrect information about him was provided in a search).

139. *See Spokeo, Inc.*, 136 S. Ct. at 1549 (emphasis added) (explaining sometimes plaintiff's risk of intangible harm may qualify as sufficient for Article III standing); *see also In re OPM Litig.*, 928 F.3d at 55–56 (explaining types of future injuries plaintiffs allege and exploring support for them).

must be "concrete," it did not intend to require them to be "tangible."[140] For example, data breach plaintiffs may allege specific instances of misuse that have already occurred.[141] Unlike the plaintiffs in *Spokeo, Inc.*, this fact helps plaintiffs with data breach claims to illustrate their *risk* of real harm is substantial.[142]

In data breach cases such as *In re OPM Litigation*, the risk at issue is one that Congress intended to remedy.[143] In recent years, Congress has shown that it intends organizations to be held accountable for their roles in data breaches, as evidenced by the representatives' comments proposed legislation.[144] Therefore, the findings of the D.C. Circuit further align with the Supreme Court's holding in *Spokeo, Inc.* because the court recognizes data breach victims' risk of real harm as one Congress intends to remedy.[145] While there is no comprehensive framework for finding liability in data breach cases, there are statutes and regulations that apply to certain facets of data breach issues.[146] This illustrates Congress's intent to provide some remedies to those impacted by breaches.[147]

---

140. *See Spokeo, Inc.*, 136 S. Ct. at 1549 (explaining what "concrete" injury may consist of in order to sufficiently meet elements of Article III standing, and acknowledging intangible harm may, at times, be "concrete"); *see also* Lorio, *supra* note 13, at 88–89 (discussing Supreme Court's reasoning as to what constitutes "concrete").

141. *See In re OPM Litig.*, 928 F.3d at 56 (explaining there were already instances of misuse of some plaintiffs' information, including unauthorized accounts and false tax returns, and noting this fact was sufficient to give rise to inference that others would likely experience fraud and misuse).

142. *Compare id.* at 56 (explaining nature of plaintiffs' alleged injuries and specific harms that have occurred), *with Spokeo, Inc.*, 136 S. Ct. at 1544–46 (discussing plaintiff's allegations of injury and questioning whether any harm occurred besides a procedural violation).

143. *See* Taryn Elliott, Comment, *Standing a Chance: Does* Spokeo *Preclude Claims Alleging the Violation of Certain State Data Breach Laws?*, 49 SETON HALL L. REV. 233, 245–46 (2018) (describing recent comments by legislators and proposed legislation after data breaches shows Congress intends to provide a remedy to affected plaintiffs); *see also* Kim, *supra* note 25, at 552–53 (noting various federal laws hold organizations accountable for data breaches).

144. *See* Elliott, *supra* note 143, at 245 (explaining recent reactions to data breaches indicating Congress intends to impose remedy for data breaches). In light of a recent Equifax breach, one senator noted that Equifax's conduct was "outrageous." *See id.* (quoting Press Release, Sen. Bob Menendez, What You Should Know About Equifax Data Breach (Sept. 14, 2017)). Further, a member of the House of Representatives commented that Equifax should have been ready to respond to the breach immediately. *See id.* Additionally, the article notes there have been many efforts to enact a federal statute regulating data breaches, such as the proposed Personal Data Notification and Protection Act. *See id.*

145. *See Spokeo, Inc.*, 136 S. Ct. at 1549–50 (holding where there is "risk of real harm," "concreteness" may be satisfied if plaintiffs can show their harm is one Congress intends to remedy).

146. *See* Kim, *supra* note 25, at 551–53 (discussing lack of a consumer-oriented federal framework for data breach litigation and how lack of framework impacts cases); *see also* Elliott, *supra* note 143, at 245 (describing reactions from federal legislators to lack of overarching federal legal remedy for data breaches).

147. *See* Elliott, *supra* note 143, at 245 (discussing facts showing congressional intent to hold organization accountable for role in data breaches). For a further discussion of these indicators of congressional intent, see *supra* Section V.A.

B. *Plaintiffs' Claims Must be Recognized to Hold Companies Accountable for Data Breaches*

If a federal court finds that the plaintiff does not have standing, it must dismiss the case immediately.[148] As a result, the court will not hear the merits of the claim.[149] This means the legal issue that the plaintiff alleges will not be decided.[150] Under the ruling from *In re OPM Litigation*, an organization that was subject to a data breach may be held liable and plaintiffs' claim may be assessed on the merits.[151] Plaintiffs sought redress due to a failure to conform to industry standards and failure to adequately protect security credentials.[152] The court found the plaintiffs had sufficient standing and, as a result, the case was remanded to be heard on its merits and potentially hold the OPM accountable.[153]

Organizations and companies are far less likely to be held accountable for their roles in data breaches if lawsuits where an increased risk of future identity theft is the only injury alleged are dismissed before court reaches the merits.[154] Plaintiffs in data breach cases bring claims under a variety of theories, including "'negligence, breach of contract, unjust enrichment, breach of fiduciary duty, unfair and deceptive business practices, invasion of privacy,' and violations of various state and federal statutes."[155] Under these theories, entities can at times be held liable for their role in a data breach.[156]

However, accountability under these theories can be imposed only if plaintiffs can surmount Article III standing requirements.[157] Federal courts should recognize the increased risk of future identity theft as injury sufficient to satisfy the standing

148. *See* Benjamin C. West, Note, *No Harm, Still Foul: When an Injury-in-Fact Materializes in a Consumer Data Breach*, 69 HASTINGS L.J. 701, 704 (2018) (explaining necessary Article III standing requirements in federal court cases). Federal courts must dismiss cases when plaintiffs do not have standing to ensure that courts are properly within their limited role and do not provide advisory opinions. *See id.*

149. *See* Galbraith, *supra* note 29, at 1375–76 (explaining impact of case being dismissed due to lack of standing on merits of case); *see also* Emily Marcum, Comment, *Corporate Liability for Data Breaches: Will Equifax Victims Have a Leg to Stand on?*, 18 WAKE FOREST J. BUS. & L. 525, 533 (2018) (noting court will not consider merits of case when plaintiff fails to meet all standing requirements).

150. *See* Lorio, *supra* note 13, at 128 (explaining many courts do not reach merits of cases in data breach litigation unless plaintiff's information has already been misappropriated).

151. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 75 (D.C. Cir. 2019) (holding plaintiffs sufficiently alleged standing and remanding case).

152. *See id.* at 51 (discussing plaintiffs' theories of OPM liability for data breach). Plaintiffs allege that both OPM and KeyPoint should have been on notice that their security defenses were insufficient. *See id.* For a further discussion of Plaintiff's theories of OPM liability for the data breach, see *supra* Part III.

153. *See id.* at 75.

154. *See* Marcum, *supra* note 149, at 555 (discussing how failing to view increased risk of identity theft as injury sufficient for Article III standing affects corporate liability).

155. Wynhausen, *supra* note 34, at 307 (quoting Megan Dowty, Note, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017)) (noting legal theories plaintiffs have brought data breach claims under).

156. *See* H. Dennis Beaver, *What Is My Liability for a Data Breach?*, KIPLINGER (June 19, 2019), https://www.kiplinger.com/article/business/T048-C032-S014-what-is-my-liability-for-a-data-breach.html [https://perma.cc/Y4QM-A5HE] (discussing how civil liability for data breach can be imposed). Courts can impose liability on an organization if it negligently protects stored information or fails to sufficiently reduce harm and notify individuals after a security breach *See id.*

157. *See* Lorio, *supra* note 13, at 128 (explaining detrimental effects of dismissing a data breach claim at standing phase).

elements so there will be far more opportunities to examine organizations' security practices.[158] If courts fail to recognize standing in these situations, the risk stemming from the data breach primarily impacts consumers rather than the companies obligated to protect their data.[159] The holding of *In re OPM Litigation* continues to move the analysis in the right direction because it recognizes the range of injuries plaintiffs often face and allows courts to examine the merits of their claims.[160] This holding is necessary, because movement in this direction can increase the risk of liability that entities face and incentivize them to better protect and manage personal information.[161]

### C. *Statutory Standing and Private Causes of Action Are Unlikely to Allow Plaintiffs to Reach the Merits of their Claims*

Conferring statutory standing is unlikely to provide plaintiffs with a way to hold companies accountable. Article III requirements are a "hard floor" and Congress may not circumvent them entirely.[162] The fact that a statute describes a right will not allow a plaintiff to sue in the absence of injury.[163] The Supreme Court has

158. *See* Marcum, *supra* note 149, at 533 (explaining plaintiffs must satisfy Article III standing requirements before liability can be imposed); Lorio, *supra* note 13, at 128 (acknowledging courts cannot hear merits unless standing is established); *see also* Kim, *supra* note 25, at 575–76, 581 (asserting that finding injury and allowing plaintiffs to proceed in more suits will lead to increased company accountability); Martin, *supra* note 19 (noting increased findings of standing may cause companies to better protect data to avoid litigation examining their practices).

159. *See* Brandon Faulkner, Note, *Hacking Into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1100–01 (2007) (explaining how risk stemming from data breaches impacts consumers); see also Braunstein, *supra* note 27, at 105 (noting "consumers bear the brunt of the harm" after data breaches).

160. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 50, 59–61 (D.C. Cir. 2019) (discussing various injuries plaintiffs alleged and holding injuries satisfied elements of Article III standing). Plaintiffs alleged harms ranging from instances of fraud to costs incurred as an attempt to mitigate risks. *See id.* at 50, 52. In this case, plaintiffs' claims were allowed to move forward so the court could examine whether OPM and Keypoint took reasonable steps to protect consumer data. *See id.* at 75.

161. *See* Michelle R. King, Note, *Restricting the Corporate Practice of Medicine: Subverting ERISA to Hold Managed Care Organizations Accountable for Health Care Treatment Decisions—the Texas Initiative*, 23 DEL. J. CORP. L. 1203, 1235–36 (1998) (noting adequate legal remedy to injured parties may increase accountability); *see also* Kim, *supra* note 25, at 575–76, 581 (explaining why increased finding of standing will incentivize better corporate practices); Martin, *supra* note 19 (noting "positive feedback loop" may occur if plaintiffs more often have standing). Given that "2019 was the most expensive year on record" for data breaches, other motivators such as increased expense, loss of business, and poor media attention are not likely to incentivize businesses to improve their data protection methods. *See* Isaac Kohen, *Data Breaches and Security 2020: Five Steps SMBs Can Take to Protect Their Data*, FORBES (Jan. 28, 2020, 8:30 AM), https://www.forbes.com/sites/theyec/2020/01/28/data-breaches-and-security-2020-five-steps-smbs-can-take-to-protect-their-data/#78b7654d75f6 [https://perma.cc/Q84H-Q6C7] (discussing losses due to data breaches in 2019).

162. *See* Dowty, *supra* note 26, at 697 (quoting Summers v. Earth Island Inst., 555 U.S. 488, 497 (2009)) (describing Supreme Court jurisprudence finding Congress may not grant standing where plaintiff cannot show injury).

163. *See id.*; Lorio, *supra* note 13, at 114.

recognized that standing requirements bind both Congress and federal courts.[164] Congressional legislation may authorize litigation by conferring standing within Article III's confines.[165] Nevertheless, litigants are required to show "a distinct and palpable injury to [themselves]" that the court can remedy.[166] Congress may not direct federal courts to hear cases where Article III standing is not met.[167]

Further, state data breach laws have not consistently conferred standing where plaintiffs could not meet Article III injury requirements.[168] Even where there is a state data breach statute theoretically creating a cause of action, plaintiffs yield inconsistent results in establishing standing.[169] This inconsistency emphasizes the need for courts to recognize a risk of future identity theft as sufficient injury satisfy standing requirements.[170]

Federal district courts in California have declined to confer standing—even where procedural violations of statutes were alleged—because plaintiffs did not establish that defendant's violation of consumer protection statutes caused injury.[171] Similarly, federal district courts in Maryland have found a lack of standing in claims brought under the Maryland Consumer Protection Act and District of Columbia Consumer Protection Procedures Act because plaintiffs did not allege sufficient injury—even in light of a statutory violation.[172] Further, federal district courts in Ohio have failed to confer standing on plaintiffs alleging violations of the Fair Credit Reporting Act because they did not allege an injury other than a statutory violation.[173] The dispositive issue in establishing standing in data breach cases is whether the court will recognize plaintiffs' increased risk of future theft as a sufficiently imminent injury under Article III, and not whether a statute confers standing in its text.[174] Therefore, a statutory cause of action alone will not confer standing on plaintiffs in

164. *See* John G. Roberts, *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1226 (1993) (illustrating impact constitutional limitations have on branches of government). "Neither the Administrative Procedure Act, nor any other congressional enactment, can lower the threshold requirements of standing under Art. III." Valley Forge Christian College v. Americans United for Separation of Church & State, 454 U.S. 464, 488 n.24 (1982) (first citing Gladstone, Realtors v. Village of Bellwood, 441 U.S. 91, 100 (1979); then citing Warth v. Seldin, 422 U.S. 490, 501 (1975)).

165. *See* Roberts, *supra* note 164, at 1226 (explaining role Congress may play in conferring standing).

166. *Id.* (internal quotation marks omitted) (quoting *Gladstone, Realtors*, 441 U.S. at 100) (noting some constitutional limitations on Congress's ability to confer standing).

167. *See id.*

168. *See* Marcum, *supra* note 149, at 554 (noting circuit split leaves victims' chances of remedy uncertain); *see also* Kim, *supra* note 25, at 551 (noting state data breach laws are not uniform).

169. *See* Dowty, *supra* note 26, at 700.

170. *See* Kim, *supra* note 25, at 551–55 (explaining the numerous statutes and regulations governing data breaches, and asserting they are confusing); *see also* Marcum, *supra* note 149, at 554 (explaining conflicting interpretations of injury in fact result in unpredictable outcomes for plaintiffs).

171. *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1218 (N.D. Cal. 2014).

172. *See* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) (finding plaintiff allegation that data breach victims were more likely to face risks of identity theft insufficient because they failed to allege hacker intent to misuse information or actual theft).

173. *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 653, 656–57 (S.D. Ohio 2014), *rev'd*, 663 Fed. App'x 384, 389 (6th Cir. 2016) (finding no standing where plaintiffs failed to show injury resulting from statutory violation).

174. *See* Roberts, *supra* note 164, at 1226 (explaining Congress may not confer standing to plaintiffs by statute where they cannot show Article III standing).

the absence of Article III injury, leaving plaintiffs unable to hold the companies who are responsible for maintaining their sensitive data accountable.[175]

Further, the Supreme Court in *Spokeo, Inc.* held that a statute could not confer Article III standing without a cognizable injury even where there was a technical statutory violation.[176] The Court rejected the contention that a violation of the Fair Credit Reporting Act conferred standing where information, the veracity of which was protected by the Act, was reported incorrectly because of a procedural violation.[177] The Court reiterated that concrete injury is required by Article III and a statutory violation alone is not enough.[178] Therefore, plaintiffs may not "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[179] However, the Court acknowledged that a risk of real harm may still satisfy the concreteness requirement for injury.[180]

The Court noted that the circuit court below did not adequately examine whether an Article III injury resulted from the procedural violation.[181] This shows that a plaintiff's ability to sue depends on whether the plaintiff can allege sufficient injury even where there may be a procedural violation of a statute. Therefore, courts should recognize an increased risk of identity theft as sufficient risk to show injury in data breach cases because in many courts, a statutory violation alone leaves plaintiffs unable to reach the merits of their claims against companies responsible for the safekeeping of personal information.[182]

## VI. THE LASTING IMPACT OF *IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION*

The FBI reports as many as 900 complaints of cybercrime each day.[183] Data breaches continue to impact billions of individuals each year and cost millions to rectify.[184] Moreover, data breaches are extremely expensive.[185] These costs include

175. *See id.* (noting statute may not provide standing where no injury exists); *see also* Kim, *supra* note 25, at 581 (explaining why standing may hold companies accountable for failure to protect information).

176. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).

177. *See id.* at 1546.

178. *See id.* at 1549 (explaining constitutional requirements of Article III standing still control even where statute is violated).

179. *See id.* at 1549–50 (citing Summers v. Earth Island Inst., 555 U.S. 488, 496 (2009) (noting plaintiff's allegations do not comport with Article III standing requirements).

180. *See id.* at 1549.

181. *See id.* at 1550 (explaining circuit court's shortcomings in determining whether Article III standing requirements were satisfied).

182. *See* Dowty, *supra* note 26, at 700. For a further discussion of courts failing to find injury in data breach cases, see *supra* Section II.C.

183. *See Report Shows Cyber-Enabled Crimes and Costs Rose in 2018*, *supra* note 11 (explaining frequency of cybercrimes).

184. *See* Snider, *supra* note 28.

185. *See* Christina Cardoza, *Report: The Costs of Data Breaches Are Rising*, SD TIMES (July 24, 2019), https://sdtimes.com/security/report-the-cost-of-data-breaches-are-rising/ [https://perma.cc/3KNX-HXTW] (explaining recent trends in data breach impact). The cost of data breaches increased 12% from 2014 to 2019. *Id.* As of 2019, each breach cost an average of $3.92 million. *Id.*

identity theft and tax fraud.[186] As a result of a data breach, victims often can be negatively impacted for years, or even decades.[187] Crucially, there are many instances where a victim of identity theft will not know of the damage they have suffered until a loan or credit card application is denied years later.[188]

Currently, the District of Columbia Circuit is one among only a handful of circuits willing to grant standing where the injury alleged is based on the increased risk of future identity theft.[189] Plaintiffs who had their personal information compromised in a data breach and face an increased risk of identity theft may only bring their claims in some areas of the country.[190] The District of Columbia Circuit's opinion, however, supports a necessary step in the way courts treat injury in fact in data breach litigation.[191] *In re OPM Litigation* recognized that courts can interpret the standing doctrine to recognize injuries faced by data breach victims while comporting with Supreme Court precedent.[192] If other courts do not adopt this approach, government and organizational security practices are less likely to change because they have less incentive to better protect against breaches.[193]

---

186. *See Data Breach: Tax-Related Information for Taxpayers*, IRS, https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers [https://perma.cc/Q5JT-L2NE] (last visited Sept. 20, 2020) (discussing relationship data breaches can have to tax-related identity theft); *see also* Hsu, *supra* note 2 (discussing impact of identity theft resulting from data breaches).

187. *See* Andrew Soergel, *Equifax Data Breach Could Have 'Decades of Impact'*, U.S. NEWS (Sept. 8, 2017), https://www.usnews.com/news/articles/2017-09-08/equifax-breach-could-have-decades-of-impact-on-consumers [https://perma.cc/429F-9GR6] (explaining impact data breaches may have on affected consumers).

188. *See Identity Theft Protection*, MICH. DEPT. OF ATT'Y GEN., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-455904—,00.html [https://perma.cc/V8M3-PR5U] (last visited Oct. 3, 2019) (noting many victims not aware of identity theft until years later).

189. *See, e.g.*, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 59 (D.C. Cir. 2019) (finding plaintiffs' risk of future injury satisfied standing requirements); Attias v. CareFirst, Inc., 865 F.3d 620, 629–630 (D.C. Cir. 2017) (finding sufficient injury to satisfy standing where victims alleged facts supporting inference of increased risk of future fraud); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 389 (6th Cir. 2016) (finding plaintiffs alleged injury for standing where data was clearly stolen with criminal intent of fraud).

190. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (holding requirements for standing were not met when plaintiffs could not show their information was misused, noting an increased risk of theft was speculative); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding any alleged future injury was speculative, and therefore insufficient for Article III standing); *see also* Marcum, *supra* note 149, at 554 (explaining standing analysis's conflicting interpretations of injury in fact lead to unpredictable data breach litigation results).

191. *See* Lorio, *supra* note 13, at 128 (explaining failure of courts to find "injury suitable [for] judicial resolution" when plaintiffs allege risk of future injury); *see also* Kim, *supra* note 25, at 550 (recognizing failure of courts to remedy victims' data breach claims).

192. *Compare* Galbraith, *supra* note 29, at 1375–77 (summarizing history and development of traditional standing doctrine), *with* Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, BUS. L. TODAY (July 17, 2018), https://businesslawtoday.org/2018/07/emerging-legal-issues-data-breach-class-actions/ [Permalink unavailable] (explaining data breach standing as new and evolving area of law pushing limits of standing doctrine).

193. *See* Marcum, *supra* note 149, at 555 (discussing impact of failing to allow plaintiffs alleging an increased risk of future identity theft to bring claims). Further, it is unlikely that allowing data breach plaintiffs alleging a risk of future harm to proceed will produce an influx of litigation if courts adhere to *Spokeo Inc.*'s guidance and limit standing to those who can show a concrete risk of harm. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016). For a further discussion of concrete injury for standing purposes, see *supra* Section V.A.