Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches

*Michael Hopkins**

TABLE OF CONTENTS

I. INTRODUCTION

In January 2014, the retailer Neiman Marcus revealed it was the target of a

* J.D. Candidate, University of the Pacific, McGeorge School of Law, to be conferred May 2019; B.A., History, University of California, Los Angeles, 2013. First of all, thank you to my friends and family, especially Hayley Graves, for their continued guidance, support, and encouragement. I also thank Professor Dajani for his time and effort as faculty advisor to this Comment. Finally, thank you to the *Law Review* staff for their advice and assistance with this Comment.

data breach affecting over one million customers' credit and debit cards.[1] Hackers had installed malware on payment terminals and stole customers' payment card information over a two-and-a-half month period.[2] Investigators found fraudulent usage on thousands of credit and debit cards accessed in the breach.[3]

In March 2014, Hilary Remijas, an affected Neiman Marcus customer, sued the retailer in a class action lawsuit over the data breach.[4] The complaint's allegations included breach of implied contract and violation of data breach laws.[5] Their alleged harm included fraudulent charges, the increased risk of identity theft due to the exposure of their private information, and time spent monitoring financial accounts to watch for potential identity theft.[6]

A federal district judge dismissed the lawsuit in 2014 for lack of Article III standing.[7] However, the Court of Appeals for the Seventh Circuit reversed and held the plaintiffs sufficiently alleged standing.[8] The Seventh Circuit found the increased risk of identity theft and the time and effort to protect against that risk conferred standing.[9] With the lawsuit allowed to continue, Neiman Marcus ultimately settled for 1.6 million dollars in 2017.[10]

The grocery store chain SuperValu faced a similar situation to Neiman Marcus when a hacker broke into the chain's databases and stole customers' payment card information.[11] Similar to Remijas, affected SuperValu customers brought class action suits alleging tort and contract claims and violation of state consumer protection and data breach notification laws.[12] Also like Remijas, the plaintiffs claimed they faced an increased risk of identity theft necessitating measures to guard against that risk, including monitoring financial accounts to look for possible identity theft.[13] The district court, in that case, dismissed the plaintiffs' claims finding no injury to support standing.[14]

---

1. Elizabeth A. Harris, Nicole Perlroth & Nathaniel Popper, *Neiman Marcus Data Breach Worse Than First Said*, N.Y. TIMES (Jan. 23, 2014), https://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html (on file with *The University of the Pacific Law Review*).

2. *Id.*

3. *Id.*

4. Suevon Lee, *Neiman Marcus to Pay $1.6M in Shopper Data Breach Suit*, LAW360 (Mar. 17, 2017), https://www.law360.com/articles/903573/neiman-marcus-to-pay-1-6m-in-shopper-data-breach-suit (on file with *The University of the Pacific Law Review*).

5. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690–91 (7th Cir. 2015).

6. *Id.* at 692.

7. *Id.* at 691.

8. *Id.* at 697.

9. *Id.* at 693, 696.

10. Lee, *supra* note 4.

11. *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 766 (8th Cir. 2017).

12. *Id.* at 767.

13. *Id.* at 769, 771.

14. *Id.* at 767.

On appeal, the Eighth Circuit found the plaintiffs' risk of future harm insufficient to confer standing.[15] The court looked to a government report on identity theft, which found the vast majority of data breaches do not lead to identity theft or fraud.[16] Based on the report, the court found it unlikely plaintiffs would suffer payment card fraud and therefore the risk of future harm was inadequate for standing.[17] The court also held the costs expended guarding against fraud insufficient because safeguarding against a speculative threat does not confer standing.[18]

The Neiman Marcus and SuperValu data breaches are examples of data breaches over the past decade that have affected millions of Americans.[19] With data breaches on the rise, the number of consumers affected will likely increase.[20] The type of information stolen varies; some data breaches affect credit card and debit card information,[21] others involve more sensitive information, such as Social Security numbers or medical histories.[22] Additionally, while some of these breaches affect national retailers,[23] hackers also target small businesses,[24] which may present an easier target because of lesser data protection safeguards.[25] The consequences of any breach vary, but can include fraudulent payment card usage

15. *Id.* at 771.

16. *Id.*

17. *Id.*

18. *Id.*

19. *See* Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers Were Hit by December Data Breach*, WASH. POST (Jan. 10, 2014), https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html (on file with *The University of the Pacific Law Review*) (explaining the data breach affecting Target in which hackers stole the credit card and debit card information of up to 40 million customers); Tara Siegal Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html (on file with *The University of the Pacific Law Review*) (detailing the Equifax cyberattack in which hackers accessed "data that potentially compromised sensitive information for 143 million American consumers").

20. *See Data Breaches in U.S. Allegedly Increasing at Record Pace*, BLOOMBERG BNA (July 24, 2017), https://www.bna.com/data-breaches-us-b73014462190/ (on file with *The University of the Pacific Law Review*) (noting 29 percent in data breaches in the first half of 2017 compared to the first half of 2016).

21. Yang & Jayakumar, *supra* note 19.

22. Siegal Bernard et al., *supra* note 19.

23. Nandita Bose, *Home Depot Confirms Security Breach Following Target Data Theft*, REUTERS (Sept. 8, 2014), https://www.reuters.com/article/us-usa-home-depot-databreach/home-depot-confirms-security-breach-following-target-data-theft-idUSKBN0H327E20140909 (on file with *The University of the Pacific Law Review*).

24. E. Scott Reckard & Tiffany Hsu, *Small Businesses at High Risk for Data Breach*, L.A. TIMES (July 4, 2014), http://www.latimes.com/business/la-fi-small-data-breaches-20140705-story.html (on file with *The University of the Pacific Law Review*).

25. Steve Strauss, *Cyber Threat Is Huge for Small Businesses*, USA TODAY (Oct. 20, 2017), https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/ (on file with *The University of the Pacific Law Review*) ("90% of small businesses [do not] use data protection").

and identity theft.[26]

These data breaches frequently lead to lawsuits.[27] While Remijas and the affected Neiman Marcus customers successfully brought their claims in federal court and ultimately reached a settlement, had the case been filed in another circuit, the result could be different.[28] Circuits are split with one side adopting the Seventh Circuit's approach in *Remijas* and the other adhering to the Eighth Circuit's reasoning in *SuperValu*.[29]

Although the Supreme Court issued a 2016 decision discussing the injury requirement of standing, the ruling in *Spokeo, Inc. v. Robins* failed to resolve the circuit split.[30] In 2017 alone, the D.C. Circuit found the increased risk of identity theft due to data breaches constituted a sufficient injury for standing, but the Fourth and Eighth Circuits held that risk insufficient.[31]

This Comment argues the Supreme Court should adopt the approach used by the Courts of Appeals finding standing.[32] Alternatively, Congress could resolve the data breach standing issue by narrowly crafting a statute recognizing a person's interest in their personally identifiable information and the harm a data breach poses to that interest.[33] Part II discusses the Article III standing requirements in the United States Constitution as interpreted by the Supreme Court and how federal courts applied these rules to data breach cases before

---

26. 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/ (on file with *The University of the Pacific Law Review*).

27. *See Lawsuits Against Equifax Pile Up After Massive Data Breach*, REUTERS (Sept. 11, 2017), https://www.reuters.com/article/us-equifax-cyber-lawsuits/lawsuits-against-equifax-pile-up-after-massive-data-breach-idUSKCN1BM2E3 (on file with *The University of the Pacific Law Review*) (noting the filing of more than 30 lawsuits against Equifax in the wake of the Equifax data breach).

28. *See* Beck v. McDonald, 848 F.3d 262, 276 (4th Cir. 2017) (holding a breach of personally identifiable information stemming from theft of a medical center's laptop did not give rise to standing); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (holding a breach of credit card and debit card information leading to alleged fraudulent usage did not give rise to standing).

29. Edward R. McNicholas & Grady Nye, *D.C. Circuit Widens the Split on Standing in Data Breach Cases After Spokeo*, LEXOLOGY (Aug. 8, 2017), https://www.lexology.com/library/detail.aspx?g=7335a949-2364-4f44-9c2a-74939d5ea1da (on file with *The University of the Pacific Law Review*). The Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits have found standing in these cases, but the Second, Third, Fourth, and Eighth have not. Dominic Spinelli, *Data Breach Standing: Recent Decisions Show Growing Circuit Court Split*, AM. BAR ASS'N, https://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/data_breach_standing_recent_decisions_show_gowing_circuit_court_split.html (last visited Apr. 12, 2018) (on file with *The University of the Pacific Law Review*); *infra* Part II; *infra* Part IV.

30. McNicholas & Nye, *supra* note 29.

31. Andrew C. Glass, David D. Christensen & Matthew N. Love, *Data Breach Doubleheader: The Eighth Circuit Issues Two Decisions Addressing Boundaries of Standing in Data Breach Class Actions*, K&L GATES (Oct. 9, 2017), http://www.klgates.com/data-breach-doubleheader-the-eighth-circuit-issues-two-decisions-addressing-boundaries-of-standing-in-data-breach-class-actions-10-09-2017/ (on file with *The University of the Pacific Law Review*).

32. *Infra* Part IV.

33. *Infra* Part V.

Clapper v. Amnesty International.[34] Part III discusses two recent Supreme Court decisions regarding standing, *Clapper* and *Spokeo*.[35] Part IV discusses the growing circuit split concerning data breach standing and contends finding the future risk of harm sufficient is the better approach that the Supreme Court should adopt.[36] In the alternative, Part V proposes a law to resolve the circuit split and discusses the advantages of a statutory solution.[37] Either a Supreme Court ruling or a statutory solution can resolve this circuit split and bring certainty to the standing determination in data breach cases.[38]

II. ARTICLE III STANDING AND PRE-*CLAPPER* STANDING IN DATA BREACH CASES

Article III of the United States Constitution restricts federal courts to deciding "Cases" and "Controversies."[39] This restriction ensures the judicial branch of the federal government does not overstep its constitutional bounds by taking over powers of the legislative and executive branches.[40] To fall within the jurisdiction granted to the federal courts by the Constitution, a plaintiff must have standing.[41] Standing shows the plaintiff has a stake in the matter warranting the federal courts' jurisdiction.[42]

To demonstrate standing, the plaintiff must establish three elements: (1) an injury showing an "invasion of a legally protected interest"; (2) a causal link between the injury and the alleged conduct of the defendant; and (3) the injury is "redressab[able] by a favorable decision."[43] Additionally, the injury cannot be indefinite.[44] It must be "concrete and particularized" and "actual or imminent, not

34. *Infra* Part II. *Clapper v. Amnesty International* was a Supreme Court decision regarding injury-in-fact and the case had a significant effect on data breach litigation. 568 U.S. 398 (2013); Rebecca J. Schwartz, *New U.S. Supreme Court Decision Will Likely Impact Data Breach Litigation*, DATA SEC. L. J. (Mar. 7, 2013), https://www.datasecuritylawjournal.com/2013/03/07/new-u-s-supreme-court-decision-will-likely-impact-data-breach-litigation/ (on file with *The University of the Pacific Law Review*) (noting Clapper confirmed the high bar for finding standing on the basis of increased risk of harm in data breach cases).

35. *Infra* Part III.

36. *Infra* Part IV.

37. *Infra* Part V. While previous scholarship has discussed statutory solutions to the data breach circuit split, it has not given the language of a proposed statute. *E.g.* Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J. L. & SOC. PROBS. 79, 117 (2017) (discussing a statutory solution to the data breach circuit split, but not proposing specific statutory language).

38. *Infra* Parts IV, V.

39. U.S. CONST. art. III, § 2.

40. DaimlerChrysler v. Cuno, 547 U.S. 332, 341 (2006) (citing Raines v. Byrd, 521 U.S. 811, 818 (1997)) ("[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.").

41. Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009).

42. *Id.*

43. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

44. *Id.* at 574 (citing Mass. v. Mellon, 262 U.S. 447, 488–89 (1923)).

conjectural or hypothetical."[45] The plaintiff bears the burden of establishing standing.[46] Lack of standing means federal courts do not have subject matter jurisdiction over the case.[47]

Data breach cases present a unique problem for plaintiffs attempting to establish standing.[48] While affected companies or organizations often come forward and reveal data breaches before a plaintiff files a lawsuit,[49] stolen information is not always used maliciously.[50] Because of this uncertainty, people affected by a data breach may have difficulty demonstrating their injury is "concrete" and "actual or imminent."[51]

Even before the *Clapper* decision, in which the Supreme Court narrowed its standard for future injuries and standing,[52] federal courts diverged in finding standing for data breaches.[53] Section A discusses pre-*Clapper* data breach cases and the courts' reasoning to find standing.[54] Section B discusses pre-*Clapper* data breach cases that did not find standing and explains why the courts reached those decisions.[55]

A. Pre-Clapper Data Breach Cases Finding Standing

In *Pisciotta v. Old National Bancorp*, the Seventh Circuit held the threat of future harm relating to a data breach was a sufficient injury to establish standing.[56] Old National Bancorp ran a website where customers could submit

45. *Id.* at 560.

46. DaimlerChrysler v. Cuno, 547 U.S. 332, 342 (2006).

47. Warth v. Seldin, 422 U.S. 490, 499 (1975) (quoting Linda R.S. v. Richard D., 410 U.S. 614, 617 (1973)) ("A federal court's jurisdiction therefore can be invoked only when the plaintiff himself has suffered 'some threatened or actual injury.'").

48. *See* Robert D. Fram, Simon J. Frankel & Amanda C. Lynch, *Standing in Data Breach Cases: A Review of Recent Trends*, BLOOMBERG BNA (Nov. 9, 2015), https://www.bna.com/standing-data-breach-n57982063308/ (on file with *The University of the Pacific Law Review*) (noting defense attorneys have had success dismissing data breach cases because of plaintiffs' lack of actual harm to grant standing).

49. *See Staples Says Security Breach May Have Affected 1.16 Million Cards*, REUTERS (Dec. 19, 2014), http://www.reuters.com/article/us-staples-cybersecurity/staples-says-security-breach-may-have-affected-1-16-million-cards-idUSKBN0JX2CY20141219 (on file with *The University of the Pacific Law Review*) (explaining Staples' admission it was subject to a data breach in which credit card and debit card information may have been accessed).

50. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, IDENTITY THEFT SERVICES: SERVICES OFFER SOME BENEFITS BUT ARE LIMITED IN PREVENTING FRAUD 3 (Mar. 2017), *available at* https://www.gao.gov/assets/690/683842.pdf (on file with *The University of the Pacific Law Review*) (noting "data breaches do not necessarily result in identity theft").

51. *See id.*

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

53. 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, 1336–43 (2017).

54. *Infra* Part II.A.

55. *Infra* Part II.B.

56. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

applications for banking services, an action requiring entering personal information.[57] A hacker breached the website and accessed sensitive customer information.[58] Affected individuals brought a class action suit against Old National Bancorp and the servicer of the website, NCR Corporation, for negligence and breach of contract claims.[59] The plaintiffs alleged emotional distress and potential economic damages.[60] NCR successfully moved to dismiss the claims against it and Old National Bancorp moved for judgment on the pleadings.[61]

The district court granted the motion finding a lack of "cognizable injury."[62] On appeal, the Seventh Circuit turned to other circuit court decisions.[63] For example, the court pointed to *Sutton v. St. Jude Medical S. C., Inc.* where the Sixth Circuit held the increased risk of future health complications stemming from a defective medical device created standing.[64] Finding these toxic exposure and defective medical device cases sufficiently analogous, the *Pisciotta* court held the threat of future harm was enough of an injury to confer standing.[65]

Similar to *Pisciotta*, in *Krottner v. Starbucks Corp.*, the Ninth Circuit held the higher risk of identity theft stemming from a data breach was a sufficient injury to confer standing.[66] In *Krottner*, an unknown thief stole a Starbucks laptop containing personally identifiable information from nearly one hundred thousand Starbucks employees.[67] Affected Starbucks employees filed class action lawsuits against Starbucks, claiming negligence and breach of implied contract.[68] These plaintiffs alleged harm in the form of increased risk of identity theft and one class representative alleged an injury of anxiety and stress due to the laptop theft.[69]

The district court in *Krottner* found the plaintiffs established Article III standing.[70] The Ninth Circuit affirmed and found the anxiety and stress injury was sufficient to confer standing before turning to the other alleged harm.[71] The court stated increased risk of identity theft was a "credible threat of real and

57. *Id.* at 631.
58. *Id.* at 632.
59. *Id.*
60. *Id.*
61. *Pisciotta*, 499 F.3d at 632.
62. *Id.*
63. *Id.* at 634.
64. *Id.* at 634 n.3; Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005).
65. *Pisciotta*, 499 F.3d at 634.
66. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).
67. *Id.* at 1140.
68. *Id.* at 1141.
69. *Id.* at 1142.
70. *Id.* at 1141.
71. *Krottner*, 628 F.3d at 1142.

immediate harm" that was not "conjectural or hypothetical."[72] In reaching this conclusion, the Ninth Circuit examined its prior decisions allowing future harm to confer standing in environmental claims.[73]

Then the court looked at other Courts of Appeals, specifically the Sixth and Seventh Circuits.[74] Viewing favorably the Seventh Circuit's holding that future harm can confer standing in *Pisciotta*,[75] the Ninth Circuit held the affected Starbucks employees had standing due to the risk of future identity theft.[76] Despite multiple circuit courts finding standing in data breach litigation, other courts reached the opposite conclusion.[77]

B. Pre-Clapper Data Breach Cases Not Finding Standing

In *Amburgy v. Express Scripts, Inc.*, the United States District Court for the Eastern District of Missouri found the increased possibility of identity theft insufficient for standing purposes despite a data breach.[78] There, a hacker infiltrated Express Scripts' database and accessed personal information before threatening to make the information public.[79] John Amburgy, an affected individual, brought a class action lawsuit against Express Scripts alleging negligence, contract violations, and other state law violations.[80] Like the *Pisciotta* and *Krottner* plaintiffs, Amburgy alleged an increased risk of fraud and crime after the breach, as well as damages for the time and money spent protecting against potential crimes.[81] Express Scripts then moved to dismiss the case, claiming the court did not have subject matter jurisdiction because Amburgy did not have standing.[82]

After reviewing the requirements for standing, the court noted the federal courts were split in finding the future risk of identity theft sufficient for standing.[83] The court addressed *Pisciotta*'s holding that found standing, but it expressed reluctance to follow a "recent trend" given standing's constitutional basis.[84] Turning to the plaintiff's allegations, the court determined Amburgy's alleged injury was not imminent because he failed to show if and/or when a

72. *Id.* at 1143.

73. *Id.* at 1142 ("[I]n the context of environmental claims, a plaintiff may challenge governmental action that creates 'a credible threat of harm' before the potential harm . . . has occurred.").

74. *Id.* at 1142–43.

75. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

76. *Krottner*, 628 F.3d at 1143.

77. *Infra* Part II.B.

78. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009).

79. *Id.* at 1049.

80. *Id.* at 1048–49.

81. *Id.* at 1049.

82. *Id.*

83. *Amburgy*, 671 F. Supp. at 1050.

84. *Id.* at 1051.

criminal would maliciously use his personal information.[85] Thus, the court labeled Amburgy's alleged injury speculative and uncertain, lacking the concrete nature required for standing.[86] Therefore, the court dismissed the case for lack of subject matter jurisdiction.[87]

A similar breach of personal and financial information occurred in *Reilly v. Ceridian Corp.*, where the Third Circuit held that an increased risk of identity theft was a hypothetical injury and therefore insufficient to confer standing.[88] There, Ceridian, a payroll company, stored social security numbers, birthdates, and other sensitive information for its customers' employees.[89] In December 2009, a hacker accessed the information of 27,000 employees.[90] Later in October 2010, affected employees filed a class action suit against Ceridian for negligence, contract, and breach of statutory violations.[91] Similar to *Krottner*, the plaintiffs alleged an increased risk of identity theft, along with costs for monitoring their credit.[92] The district judge granted Ceridian's motion to dismiss on the ground the plaintiffs lacked standing.[93]

On appeal, the Third Circuit affirmed the lower court's ruling.[94] The court held that until the hacker used the personal information maliciously, "no misuse of the information, and thus, no harm" occurred.[95] Although the court recognized future injuries can confer standing if they are imminent, it found the plaintiffs' injuries were too conjectural to be imminent.[96] In particular, the court noted future identity theft would depend on circumstances such as "if the hacker attempt[ed] to use the information, and if he d[id] so successfully."[97]

The Third Circuit then criticized the "skimpy rationale" of the *Pisciotta* and *Krottner* decisions.[98] The *Reilly* court stated comparisons to environmental cases, as done in *Krottner*,[99] were inappropriate.[100] The court criticized these comparisons because in environmental suits monetary compensation "may not adequately return plaintiffs to their original position," but data breach defendants

85. *Id.* at 1052.

86. *Id.*

87. *Id.* at 1058.

88. Reilly v. Ceridian Corp., 664 F.3d 38, 40, 42 (3d Cir. 2011).

89. *Id.* at 40.

90. *Id.*

91. Reilly v. Ceridian Corp., No. 10–5142, 2011 WL 735512, at *2 (D.N.J. Feb. 22, 2011), *aff'd*, 664 F.3d 38 (3d Cir. 2011).

92. *Reilly*, 664 F.3d at 40.

93. *Id.* at 41.

94. *Id.* at 46.

95. *Id.* at 42.

96. *Id.* at 43.

97. *Reilly*, 664 F.3d at 43.

98. *Id.* at 44.

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

100. *Reilly*, 664 F.3d at 45.

can easily recompense for identity fraud with monetary compensation.[101] With a growing circuit split, the stage was set for the Supreme Court to lay down guidance on the issue.[102]

III. THE SUPREME COURT WEIGHS IN: *CLAPPER* AND *SPOKEO*

In 2013, the Supreme Court handed down a 5-4 decision in *Clapper v. Amnesty International USA*.[103] Although *Clapper* concerned constitutional privacy, its effect on the standing doctrine had a large impact on data breach cases.[104] Section A discusses the *Clapper* opinion and its effect on standing requirements.[105] Section B discusses the *Spokeo* ruling and how it affected standing rules.[106]

A. *Clapper and the Strict Requirements for Standing*

In 2008, Congress enacted the FISA Amendments Act of 2008 changing how the government could surveil foreign individuals.[107] Various individuals and organizations, such as attorneys and human rights groups, challenged the law and claimed it would subject their communications with foreign individuals to United States government surveillance.[108] Those challenging the law made two arguments regarding the injury required for standing: (1) the likelihood the government would surveil their communications under the law, and (2) costs spent to protect against government interception of communications.[109]

At the district court level, the judge granted the government's motion for summary judgment, holding those challenging the law lacked standing.[110] The Second Circuit reversed the district court, finding alleged future injuries "sufficiently likely" to create standing.[111]

After examining the prior decisions on the case, the Supreme Court turned to the legal requirements for standing.[112] The Court reiterated its rule that "an injury

101. *Id.* at 45–46.

102. *Infra* Part III.

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

104. *See* Douglas Meal & David Cohen, *How High Court's Clapper Ruling Will Impact Breach Cases*, LAW360 (Mar. 5, 2013), https://www.law360.com/articles/420896/how-high-court-s-clapper-ruling-will-impact-breach-cases (on file with *The University of the Pacific Law Review*) (noting the *Clapper* opinion will likely help data breach defendants dismiss cases against them).

105. *Infra* Part III.A.

106. *Infra* Part III.B.

107. *Clapper*, 568 U.S. at 404.

108. *Id.* at 406.

109. *Id.* at 407.

110. *Id.*

111. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011), *rev'd*, 568 U.S. 398 (2013).

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

must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[113] Further, the Court added that standing inquiries are "especially rigorous" when they involve separation of powers or national security issues.[114] It then stated the injury must be "certainly impending" to confer standing and that allegations of possible future injury were insufficient.[115]

Applying these requirements, the Court held the respondents' first argument—that the government was likely to surveil their communications—relied on conjecture and possibilities, not enough to be certainly impending.[116] The opinion noted surveillance of respondents' communications would require the government to target respondents' foreign contacts using the challenged law.[117] Thus, this potential series of events—labeled the "chain of possibilities"—was too speculative.[118] The second theory—concerning the costs spent protecting against government surveillance—was similarly insufficient because respondents took measures to avoid a harm that was not certainly impending.[119] For these reasons, the Supreme Court reversed the Second Circuit's ruling.[120]

In the opinion, the majority referenced another test for whether future harm confers standing.[121] In certain cases, the Court has held the "substantial risk" that harm will occur constitutes a sufficient injury.[122] However, the majority did not fully explore the boundaries of this other standard, except to note respondents would also fail under this standard because of the speculative nature of the harm.[123]

The majority's thorough discussion of how injuries must be "certainly impending" for standing and the placement of the "substantial risk" standard in a footnote identified "certainly impending" as the dominant rule.[124] Thus, the Supreme Court highlighted a test with a "very strict" standard.[125] This high

113. *Id.* (citing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).

114. *Id.* at 408–09.

115. *Id.* at 409.

116. *Id.* at 410.

117. *Clapper*, 568 U.S. at 411.

118. *Id.* at 414.

119. *Id.* at 416.

120. *Id.* at 422.

121. *Id.* at 414 n.5.

122. *Clapper*, 568 U.S. at 414 n.5.

123. *See id.* ("But to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here.").

124. *See id.* at 409, 414 n.5 (noting the discussion of certainly impending in the body of the opinion but pointing to how substantial risk appears in a footnote).

125. Patrick Gallagher, *Environmental Law, Clapper v. Amnesty International, USA and the Vagaries of Injury-in-Fact: "Certainly Impending" Harm, "Reasonable Concern," and "Geographic Nexus"*, 32 UCLA J. ENVTL. L & POL'Y 1, 1 (2014).

standard poses a challenge for data breach plaintiffs potentially unaware of the specifics of the breach, such as when the defendant worked to cover up the breach.[126] Additionally, under the *Clapper* standard, "certainly impending" harm may require certain events, like the hacker making an unauthorized purchase with the stolen information.[127] Because *Clapper* deemed "speculative chain[s] of possibilities" insufficient for an injury,[128] the case was problematic for data breach plaintiffs.[129]

Now armed with this powerful tool,[130] data breach defendants effectively used it to dismiss cases against them.[131] Although *Clapper* may have shifted the scales toward data breach defendants, federal courts post-*Clapper* continued to reach opposite conclusions on standing.[132] Thus, the stage was set for another Supreme Court opinion.[133]

B. *Spokeo and the Failure to Resolve the Standing Issue*

Amidst the ongoing standing question, in 2015 the Supreme Court granted certiorari for *Spokeo, Inc. v. Robins*.[134] Although it did not involve a data breach, *Spokeo* concerned how statutory violations relate to standing and the type of injury sufficient to confer standing.[135] Thus, the grant of certiorari led some to believe the Supreme Court would put the data breach standing issue to rest.[136]

---

126. *See* Gabrielle Orum Hernández, *Uber's Data Breach Cover-Up Strategy May Be More Common Than You'd Think*, CONN. L. TRIB. (Nov. 30, 2017), https://www.law.com/ctlawtribune/sites/ctlawtribune/2017/11/30/ubers-data-breach-cover-up-strategy-may-be-more-common-than-youd-think/ (on file with *The University of the Pacific Law Review*) (noting data breaches often go unreported or are often covered up).

127. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

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

129. *See Reilly*, 664 F.3d at 42 (stating unless and until certain events occurred, the data breach plaintiff had not suffered a harm).

130. Meal & Cohen, *supra* note 104.

131. Heidi J. Milicic, *Standing to Bring Data Breach Class Actions Post*-Clapper, AM. BAR ASS'N (Aug. 7, 2014), http://apps.americanbar.org/litigation/committees/commercial/articles/summer2014-0814-data-breach-class-actions-post-clapper.html (on file with *The University of the Pacific Law Review*) (noting at the time of the article's publication virtually all data breach "defendant[s] asserting a *Clapper*-based challenge ha[ve] been successful" in contesting standing).

132. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding the increased risk of harm from a data breach sufficient for standing); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (holding identity theft risk alone insufficient to confer standing).

133. *Infra* Part III.B.

134. *Spokeo, Inc. v. Robins*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/ (last visited Apr. 12, 2018) (on file with *The University of the Pacific Law Review*) (noting the Supreme Court granted the petition for certiorari on April 27, 2015).

135. Marcus A. Asner et al., *Supreme Court Expected to Decide Soon Whether to Grant Certiorari in Spokeo*, LEXOLOGY (Apr. 15, 2015), https://www.lexology.com/library/detail.aspx?g=9fd4a392-e4e2-4713-88c7-6d911829a69b (on file with *The University of the Pacific Law Review*).

136. McNicholas & Nye, *supra* note 29.

Spokeo, a consumer reporting agency, ran a "people search engine" which generated profiles containing personal information about individuals.[137] Thomas Robins accessed his own profile on Spokeo's service and found inaccuracies.[138] He brought a class action suit against Spokeo under the Fair Credit Reporting Act (FCRA) based on the incorrect information.[139] The district court dismissed the case for lack of standing, but the Ninth Circuit reversed, holding the alleged statutory violation sufficient to confer standing.[140]

The Supreme Court addressed how statutes affect standing, noting Congress' ability to make previously inadequate injuries adequate for standing purposes.[141] However, not all statutory violations give rise to standing because the injury needs to be particularized—that is, both individualized and concrete.[142] An injury is concrete if it actually exists.[143] The majority rejected the need for additional harm beyond the harm Congress specified, but maintained a mere procedural violation of a law is not enough.[144] The Court then remanded to the Ninth Circuit, directing the Ninth Circuit to discuss the concreteness requirement.[145]

Spokeo is relevant to data breach litigation because the case concerned the type of injury necessary for standing.[146] Additionally, there is greater relevance because data breach plaintiffs, similar to the *Spokeo* class, often claim statutory violations.[147] Like the plaintiffs in the *Spokeo* case, data breach plaintiffs may allege standing under violations of the FCRA.[148] Therefore, the inability of a procedural FCRA violation to confer standing may impact data breach cases implicating the statute.[149]

Despite *Spokeo*'s relevance to data breach lawsuits, the opinion did not address the "certainly impending" test and contained minimal discussion of the imminence requirement, limiting the opinion's ability to put the standing question to rest.[150] Therefore, although the Supreme Court issued an opinion on

---

137. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).

138. *Id.*

139. *Id.*

140. *Id.* at 1546.

141. *Id.* at 1549 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992)).

142. *Spokeo*, 136 S. Ct. at 1548.

143. *Id.*

144. *Id.* at 1549.

145. *Id.* at 1550.

146. *Id.* at 1548.

147. *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1049 (E.D. Mo. 2009) (noting the plaintiff's claims included "violations of 'data breach notification laws' of various States, and violations of Missouri's Merchandising Practices Act").

148. *See In re* Horizon Healthcare Services Inc. Data Breach Litig., 846 F.3d 625, 634 (3d Cir. 2017) ("All four of the named Plaintiffs argue that the violation of their statutory rights under FCRA gave rise to a cognizable and concrete injury.").

149. *See Spokeo*, 136 S. Ct. at 1549 (indicating a bare procedural violation of a statute, without any other harm, is not a sufficient injury).

150. *See generally id.* at 1540 (noting the court did not mention the "certainly impending" test and only

standing, the data breach standing circuit split continues.[151]

IV. THE CONTINUING CIRCUIT SPLIT OVER DATA BREACH STANDING AND A SUPREME COURT SOLUTION

Though the Supreme Court handed down the *Spokeo* opinion in 2016, the growing incidence of data breach litigation has since led to a sizeable circuit split.[152] Just as before *Spokeo*, the divide centers around whether the increased risk of identity theft sufficiently confers standing.[153] Section A discusses circuit courts finding standing in data breach suits post-*Spokeo* and their reasoning.[154] Section B addresses a circuit court decision rejecting standing in a data breach case post-*Spokeo* and its rationale.[155] Section C argues finding standing in data breach suits is the better approach and why the Supreme Court should so hold.[156]

A. Recent Data Breach Cases Finding Standing

In 2016, the Sixth Circuit held the increased risk of identity theft, along with costs expended to address the risk, a sufficient injury to confer standing.[157] In *Galaria v. Nationwide Mutual Insurance Co.*, hackers breached Nationwide's databases and stole over a million customers' personal information.[158] In response, affected customers spent time and money watching for identity theft.[159] Two of these customers brought separate class action lawsuits against Nationwide for FCRA violations and alleged tort causes of action.[160] The cases were later consolidated, but the district court dismissed them holding the plaintiffs lacked standing by failing to allege a cognizable injury or state a claim for relief.[161]

On appeal, the Sixth Circuit reversed the dismissal.[162] Rather than focus on *Clapper*'s "certainly impending" test,[163] the court used the "substantial risk" standard.[164] The court held the substantial risk of identity theft and fraud, along

briefly mentioned the "actual or imminent" standing requirement).

151. *Infra* Part IV.
152. *Infra* Parts IV.A–B.
153. *Infra* Parts IV.A–B.
154. *Infra* Part IV.A.
155. *Infra* Part IV.B.
156. *Infra* Part IV.C.
157. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).
158. *Id.* at 386.
159. *Id.* at 386–87.
160. *Id.* at 386.
161. *Id.* at 386–87.
162. *Galaria*, 663 F. App'x at 391.
163. *Supra* Part II.A.
164. *Galaria*, 663 F. App'x at 388.

with mitigation costs, was a cognizable injury.[165] Addressing *Clapper*, the court found no need to speculate about future injuries because hackers already had the plaintiffs' personal information.[166] Unlike *Clapper*, where the Supreme Court found the government's potential interception of plaintiffs' communications too uncertain,[167] the *Galaria* court found the targeting of personal information allowed for the reasonable inference the hackers would take malicious action.[168] Furthermore, the court distinguished *Clapper* by noting the imminence of the identity theft.[169]

A similar data breach affected the health insurer CareFirst and in the resulting case the D.C. Circuit found the substantial risk of future harm sufficient for standing.[170] Hackers accessed CareFirst's database containing customer information, such as names and social security numbers.[171] In the resulting class action, plaintiffs made several claims including, negligence and breach of contract.[172] The district court dismissed the plaintiffs' case because neither a present injury nor a likely future injury existed.[173]

The circuit court affirmed the validity of both the "certainly impending" and "substantial risk" tests.[174] Using the latter test, the court found a substantial risk of future harm arose when the hacker stole the sensitive information.[175] Similar to the *Galaria* court, the *Attias* court noted how the plaintiffs presented a greater risk of harm than in *Clapper*.[176] Unlike the *Clapper* scenario, a hacker already breached CareFirst's database making the risk of future harm more substantial and less speculative.[177] Finding a sufficient injury for standing, the court reversed the dismissal.[178]

Another data breach lawsuit forced the Ninth Circuit to determine if its holding in *Krottner* remained valid after *Clapper*.[179] In *In re Zappos.com, Inc.*, the court held *Krottner* to be reconcilable with *Clapper*.[180] In *Zappos*, hackers

165. *Id.*

166. *Id.*

167. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 411 (2013).

168. *Galaria*, 663 F. App'x at 388.

169. *Id.* at 389.

170. Attias v. Carefirst, Inc., 865 F.3d 620, 622, 629 (D.C. Cir. 2017).

171. *Id.* at 622–23.

172. *Id.* at 623.

173. *Id.*

174. *Id.* at 626–27.

175. *Attias*, 865 F.3d at 629.

176. *Id.* at 628.

177. *Id.* at 628–29.

178. *Id.* at 630.

179. Hunton & Williams, LLP, *Ninth Circuit Reverses District Court Decision in Zappos Consumer Data Breach Case*, LEXOLOGY (Mar. 23, 2018), https://www.lexology.com/library/detail.aspx?g=4c33107b-caa1-4c32-8173-b70ec7768ff6 (on file with *The University of the Pacific Law Review*).

180. *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1026 (9th Cir. 2018).

breached the defendant's servers and allegedly obtained customers' payment card information and other personal information.[181] Several affected customers filed class action lawsuits claiming inadequate protection of their personal information.[182] After consolidating the suits, the district court held the plaintiffs lacked allegations of actual identity theft.[183] Thus, the plaintiffs did not have standing and the district court dismissed their suits.[184]

The Ninth Circuit reversed the dismissal on appeal.[185] Similar to the courts in *Galaria* and *Attias*, the Ninth Circuit acknowledged the "certainly impending" standard in *Clapper* but used the "substantial risk" standard instead.[186] In holding *Krottner* valid, the court noted *Krottner* did not involve "national security or separation of powers concerns" and therefore the standing analysis was less rigorous than in *Clapper*.[187] With *Krottner* as precedent, the court held the plaintiffs' substantial risk of identity theft or fraud was a sufficient injury to confer standing.[188] While the Sixth, D.C., and Ninth Circuits found standing from the risk of identity theft post-*Spokeo*, the Fourth Circuit rejected plaintiffs' standing based on the same risk.[189]

B. A Recent Data Breach Case Not Finding Standing

The Fourth Circuit held the increased risk of identity theft stemming from a data breach too speculative to confer standing in *Beck v. McDonald*.[190] A laptop containing personal information for thousands of patients went missing from a Veterans Affairs hospital.[191] An investigation deemed it likely stolen.[192] Two patients brought a class action lawsuit alleging negligence and statutory violations.[193] At the district court level, the judge held the risk of future identity theft and measures protecting against that risk inadequate for standing.[194]

On appeal, the circuit court considered the uncertainty of whether a thief took the laptop to commit identity theft and the lack of actual identity theft allegations.[195] Therefore, the court held a risk of future harm insufficient for

181. *Id.* at 1023.
182. *Id.*
183. *Id.* at 1024.
184. *Id.*
185. *In re Zappos.com*, 888 F.3d at 1030.
186. *Id.* at 1024, 1029.
187. *Id.* at 1026.
188. *Id.* at 1029.
189. *Infra* Part IV.B.
190. Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017).
191. *Id.* at 267.
192. *Id.*
193. *Id.*
194. *Id.* at 268.
195. *Beck*, 848 F.3d at 274.

standing because that harm was speculative.[196]

Unlike some other circuit courts,[197] the *Beck* court used statistics in its holding.[198] Specifically, the plaintiffs asserted that 33% of affected patients would fall victim to identity theft, a percentage the court determined too small a figure to meet the "substantial risk" test.[199] Time and money spent on protective measures, such as credit monitoring services, failed to confer standing because the patients took these steps in response to a speculative threat.[200]

This growing circuit split identified by *Beck*[201]can lead to negative consequences, such as forum shopping; therefore, federal courts should use a singular approach to data breach standing.[202]

C. The Better Approach to Standing

The circumstances in data breach cases differ, including whether a thief stole payment card information or more sensitive data, such as social security numbers.[203] However, in all of these cases the end result is often the same—confidential information is now vulnerable and likely in the hands of criminals.[204] These data breaches can lead to severe penalties and prison time for hackers.[205] Because of the serious consequences, criminals likely do not break into databases without reason.[206] These hackers commonly sell the stolen information on the internet where the information may be bought to commit identity theft or fraud.[207] Considering these circumstances, the Supreme Court should adopt a rule establishing increased risk of identity theft and fraud as a sufficient injury for standing under the "substantial risk" standard.[208]

---

196. *Id.*

197. *Supra* Part IV.A.

198. *Beck*, 848 F.3d at 275–76.

199. *Id.*

200. *Id.* at 276–77.

201. *Id.* at 273–74.

202. COMMISSION ON REVISION OF THE FEDERAL COURT APPELLATE SYSTEM STRUCTURE AND INTERNAL PROCEDURES: RECOMMENDATIONS FOR CHANGE 13 (1975), *reprinted in* 67 F.R.D. 195, 218 (1975).

203. *See, e.g.*, *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 766 (8th Cir. 2017) (noting criminals hacked the defendant's computer network and gained access to customers' credit and debit card information); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631–32 (7th Cir. 2007) (stating a hacker breached the defendant's database containing data including customers' social security numbers).

204. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017) (noting an intruder hacked into defendant's computers and accessed a database containing the personal information of customers).

205. Christopher Coble, *What Are the Criminal Penalties for Hacking?*, FINDLAW (Feb. 2, 2016), http://blogs.findlaw.com/blotter/2016/02/what-are-the-criminal-penalties-for-hacking.html (on file with *The University of the Pacific Law Review*) (indicating federal hacking statutes often carry 10-year prison sentences).

206. *See id.* (indicating fines and prison sentences for violations of hacking laws).

207. Selena Larson, *What Cybercriminals Do with Stolen Social Security Numbers*, CNN (Sept. 19, 2017), http://money.cnn.com/2017/09/19/technology/business/equifax-breach-social-security/index.html (on file with *The University of the Pacific Law Review*).

208. Daniel Bugni, Note, *Standing Together, An Analysis of the Injury Requirement in Data Breach*

In formulating this rule, the Supreme Court should take a similar stance as the Seventh Circuit in *Remijas* and consider why hackers targeted the database.[209] "Why . . . would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[210]

Courts often reference the "speculative chain of possibilities" in *Clapper*[211] when denying standing on the basis of future harm in data breach cases.[212] The *Clapper* respondents alleged an injury requiring five contingent events before the harm occurred.[213] Unlike *Clapper*, hackers have often already accessed a database with personal information in data breach cases and now possess the sensitive data.[214] The hacker, or another criminal, need only maliciously use that stolen information for the identity theft or fraud to occur.[215] Thus, only one event needs to happen for the harm to arise.[216] This, along with the likely reason criminals hack databases,[217] presents not a "speculative chain of possibilities," but a plausible result that substantially increases the risk of identity theft or fraud.[218]

Despite *Clapper*'s focus on the "certainly impending" test,[219] federal courts have discretion in analyzing future injuries under either the "certainly impending" test or the "substantial risk" test.[220] Therefore, the Supreme Court should clarify that the "substantial risk" test applies to data breach cases.[221]

Class Actions, 52 GONZ. L. REV. 59, 90 (2016). *But see* Megan Dowty, Note, *Life Is Short: Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 702 (2017) (noting compensating data breach plaintiffs on the basis of increased risk of identity theft would require speculation).

209. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

210. *Id.*

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

212. *See* Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (finding the future harm of identity theft would not occur unless a "chain of possibilities" happened).

213. *Clapper*, 568 U.S. at 410.

214. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017) (noting an intruder hacked into defendant's computers and accessed a database containing the personal information of customers).

215. *See* Ricardo Villadiego, *The Equifax Data: Now That They Have It, How Will Hackers Use It?"*, FORBES (Nov. 29, 2017), https://www.forbes.com/sites/forbestechcouncil/2017/11/29/the-equifax-data-now-that-they-have-it-how-will-hackers-use-it/ (on file with *The University of the Pacific Law Review*) (indicating after data breach criminals will likely use stolen private information to commit identity theft).

216. *See id.* (stating after data breach hackers will likely use stolen personal data to perpetrate identity theft).

217. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (stating the likely purpose of hacking a database is to maliciously use the private information).

218. *See Attias*, 865 F.3d at 629 (finding a substantial risk of identity theft when intruders hacked into a database with confidential information).

219. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409, 414 n.5 (2013) (noting the discussion of certainly impending in the body of the opinion but pointing to how substantial risk appears in a footnote).

220. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014).

221. *See id.* (noting the "certainly impending" and "substantial risk" tests are both used for future injuries).

Unlike *Clapper*, data breach cases do not involve national security or separation of powers issues, making the standing inquiry less rigorous.[222] This less rigorous inquiry means the "substantial risk" test is appropriate for data breach cases.[223] Because a breach of private information creates a substantial risk of identity theft, the Supreme Court should hold data breaches of personal information constitute a sufficient future injury for standing.[224]

Application of the "certainly impending" test could still allow for standing as seen in *In re Adobe Systems, Inc. Privacy Litigation*.[225] In data breaches, hackers steal personal information to use it for criminal purposes; therefore, the likelihood of identity theft or fraud is much greater than the harm in *Clapper*.[226] Unlike *Clapper*, no speculation is needed to find hackers have already taken the plaintiff's personal information.[227]

Steps taken to protect against a hypothetical or speculative future harm are not considered an adequate injury.[228] However, the Supreme Court should consider holding the costs expended to safeguard against identity theft resulting from data breaches as a sufficient injury because data breaches of private information create more concrete risks of harm[229] In lieu of a Supreme Court ruling, a statute could also resolve the data breach standing issue.[230]

V. A STATUTORY SOLUTION

A statutory solution may cure the data breach standing issue by specifying an individual's interest in the confidentiality of his or her personal information and exposure of the information in a data breach harms this interest.[231] Section A discusses how statutes can establish standing.[232] Section B provides the language

222. *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1026 (9th Cir. 2018); *see also* Case Comment, *Standing—Challenges to Government Surveillance*—Clapper v. Amnesty International USA, 127 HARV. L. REV. 298, 298 (2013) ("[T]he 'certainly impending' standard . . . should only be applied to litigants challenging governmental action in foreign affairs or national security.").

223. *See In re Zappos.com*, 888 F.3d at 1029 (applying the "substantial risk" test to data breach litigation).

224. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (noting a substantial risk of harm when hackers breached a database and stole private information).

225. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014).

226. *See Remijas*, 794 F.3d at 693 (stating hackers presumably hack into databases to use the personal information for identity theft or fraud).

227. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014).

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

229. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017) (finding a substantial risk of identity theft when intruders hacked into a database with confidential information).

230. *Infra* Part V.

231. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 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.").

232. *Infra* Part V.A.

of a proposed statute.[233] Section C addresses the advantages of a statutory solution.[234]

A. Statutes and Standing

While the standing doctrine is constitutionally rooted,[235] statutes can be relevant to determine whether standing exists in a case.[236] "The actual or threatened injury required by Article III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[237] Additionally, "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."[238] Thus, Congress can make previously inadequate injuries sufficient for standing.[239]

In *In re Horizon Healthcare Services Inc.*, the Third Circuit held alleged violations of statutory rights under the FCRA were sufficient injuries for standing.[240] There, a thief stole two laptops containing the personal information, including Social Security numbers, of a health insurer's customers.[241]

The Third Circuit found "Congress established that the unauthorized dissemination of personal information by a credit reporting agency causes an injury in and of itself."[242] The court's determination rested on how Congress established a private right of action in the FCRA and the harm to be prevented by the law closely related to invasion of privacy, a traditional basis for lawsuits.[243] Thus, the Third Circuit held the alleged FCRA violations sufficient for standing purposes.[244]

In *Spokeo*, the Supreme Court indicated Congress could elevate concrete injuries into an injury-in-fact for standing.[245] Furthermore, the Court stated intangible injuries or the risk of real harm could meet the concreteness

233. *Infra* Part V.B.

234. *Infra* Part V.C.

235. Summers v. Earth Island Inst., 555 U.S. 488, 492–93 (2009).

236. Warth v. Seldin, 422 U.S. 490, 500 (1975).

237. *Id.* (quoting Linda R.S. v. Richard D, 410 U.S. 614, 617 n.3 (1973)).

238. Lujan v. Defenders of Wildlife, 504 U.S. 555, 580 (1992) (Kennedy, J., concurring).

239. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (citing Lujan, 504 U.S. at 578). An example includes the Clean Air Act's granting of a procedural right to protect a person's concrete interests. 42 U.S.C.A. § 7607(b)(1) (West 2018); Mass. v. E.P.A., 549 U.S. 497, 517–18 (2007).

240. *In re* Horizon Healthcare Litigation Services Inc. Data Breach Litig., 846 F.3d 625, 635 (3d Cir. 2017).

241. *Id.* at 630.

242. *Id.* at 639.

243. *Id.* at 639–40.

244. *Id.* at 640.

245. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992)).

requirement.[246] Data breaches bring the risk of real harm by identity theft or fraud to those affected.[247] Even though there is only a risk of harm and the exposure of personal information is intangible, data breaches can create concrete injuries that satisfy the concreteness requirement.[248] Thus, Congress could enact a statute to elevate the concrete injury, exposure of personal information in data breaches, to an injury-in-fact.[249] With guidance from cases like *Spokeo* and *In re Horizon Healthcare Services Inc.*, a statute could confer standing in data breach cases.[250]

B. Proposed Statutory Language

The following is the text of a proposed statute to end the data breach standing circuit split, taking language and influence from California's data breach notification law.[251] California's law serves as a strong starting point because it was the first data breach notification law in the United States and has served as a model followed by other states.[252] Additionally, multiple amendments over the years to California's data breach notification law means the law is still up-to-date and can act as a model for the proposed statute.[253]

(a) A person has an interest in maintaining the confidentiality of his or her personal information.[254]
(b) The interest in the confidentiality of personal information is harmed when the personal information is exposed in a data breach in accordance with subdivision (c).[255]

246. *Id.*

247. *See In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1027 (9th Cir. 2018) ("[T]he information taken in the data breach . . . gave hackers the means to commit fraud or identity theft.").

248. *See Spokeo*, 136 S. Ct. at 1549 (noting intangible injuries can be concrete and the risk of real harm can satisfy the concreteness requirement).

249. *See id.* (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992)) ("Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'").

250. *Infra* Part V.B.

251. *See generally* CAL. CIV. CODE § 1798.82 (West 2018) (noting the law's provisions to serve as a model for the proposed statute).

252. *See* Brandy L. Worden, *Understanding California's Data Breach Notification Law: Protecting Your Company & Customers*, LEXOLOGY (Aug. 11, 2017), https://www.lexology.com/library/detail.aspx?g=a18fee34-e1cb-4993-9e6c-d98fcd86f6e9 (on file with *The University of the Pacific Law Review*) ("California became the first state to enact its Data Breach Notification Law. This law has become a model that has been followed by many states across the United States.").

253. *See id.* (indicating the California Legislature has amended the California data breach notification law over the years, with the most recent changes taking effect in January 2017).

254. *See generally In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1027 (9th Cir. 2018) (noting the sensitivity of the information stolen in a data breach and how the exposed information "gave hackers the means to commit fraud or identity theft").

255. *See generally id.* (discussing the sensitivity of the information stolen in a data breach and how the exposed information "gave hackers the means to commit fraud or identity theft").

(c) The harm in subdivision (b) arises if:[256]
  (1) the personal information was stored unencrypted, or[257]
  (2) the personal information was stored encrypted, but the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person.[258]

(d) A person experiencing the harm in subdivision (b) may, either at law or in equity, in any court of competent jurisdiction, sue the individual or business maintaining the database that experienced the data breach.[259]

(e) A person bringing an action under this section against an individual may recover only the actual expenses, if reasonable under the circumstances, incurred as a result of the data breach.[260]

(f) A person bringing an action under this section against a business employing less than 100 employees may recover only the actual expenses, if reasonable under the circumstances, incurred as a result of the data breach.[261]

(g) A person harmed under this section shall be entitled to freeze their credit with credit reporting agencies at no cost within one year of the disclosure of the data breach.[262]
  (1) The costs to freeze credit under subdivision (g) shall be paid for by the individual or business maintaining the database that experienced the data breach.[263]
  (2) For purposes of subdivision (g), "credit reporting agencies" means the following credit reporting agencies:

---

256. CAL. CIV. CODE § 1798.82(a) (West 2018).

257. *Id.*

258. *Id.*

259. 15 U.S.C.A. § 77k(a) (West 2018).

260. *See generally* A.J. Dellinger, *Americans Spent $1.4 Billion on Credit Freezes After Equifax Breach*, MSN (Mar. 22, 2018), https://www.msn.com/en-us/money/markets/americans-spent-dollar14-billion-on-credit-freezes-after-equifax-breach/ar-BBKzDIZ (on file with *The University of the Pacific Law Review*) ("Americans spent an estimated $1.4 billion on credit freezes in the wake of the massive data breach at credit reporting company Equifax."); Jessica Vomiero, *Small Businesses Often More Vulnerable to Cyberattacks, Experts Say*, GLOBAL NEWS (June 30, 2017), https://globalnews.ca/news/3567122/petya-ransomware-cybersecurity-businesses/ (on file with *The University of the Pacific Law Review*) (noting the limited financial resources of small businesses to defend against cyberattacks and deal with the consequences of one).

261. *See generally* Dellinger, *supra* note 260 ("Americans spent an estimated $1.4 billion on credit freezes in the wake of the massive data breach at credit reporting company Equifax . . . ."); Vomiero, *supra* note 260 (noting the limited financial resources of small businesses to defend against cyberattacks and deal with the consequences of one).

262. CAL. CIV. CODE § 1798.82(d)(2)(G) (West 2018).

263. *Id.*

> Equifax, Experian, and TransUnion.[264]
>
> (h) For purposes of this section, "data breach" means the unauthorized access and acquisition of computerized data containing personal information.[265]
>
> (i) For purposes of this section, "personal information" means:[266]
>
> (1) A person's first name or first initial and last name in combination with one or more of the following:[267]
>
> (A) Social security number.[268]
>
> (B) Driver's license number.[269]
>
> (C) Account number or credit card or debit card number.[270]
>
> (D) Medical information.[271]
>
> (E) Health insurance information.[272]
>
> (2) A user name or email address, in combination with a password, or security question and answer, that would permit access to an online account.[273]

Through the adoption of a statute like the proposed solution, Congress could end the data breach standing circuit split.[274]

C. Advantages of a Statutory Solution

While a Supreme Court ruling could put the standing issue to rest, a federal statute would offer some benefits.[275] The statute would have to advance through the deliberative legislative process.[276] This legislative process lets stakeholders

---

264. *See* LaToya Irby, *Who Are the Three Major Credit Bureaus?*, THE BALANCE (Oct. 10, 2017), https://www.thebalance.com/who-are-the-three-major-credit-bureaus-960416 (on file with *The University of the Pacific Law Review*) (noting Equifax, Experian, and TransUnion are the three major credit reporting agencies in the United States).

265. CAL. CIV. CODE § 1798.82(g) (West 2018).

266. *Id.* § 1798.82(h).

267. *Id.* § 1798.82(h)(1).

268. *Id.* § 1798.82(h)(1)(A).

269. *Id.* § 1798.82(h)(1)(B).

270. CIV. § 1798.82(h)(1)(C).

271. *Id.* § 1798.82(h)(1)(D).

272. *Id.* § 1798.82(h)(1)(E).

273. *Id.* § 1798.82(h)(2).

274. *See supra* Part IV (noting the circuit split over standing in data breach litigation).

275. *See* Mank, *supra* note 53, at 1365 (stating Congress could pass a law providing better remedies for data breach litigants).

276. *See* VALERIE HEITSHUSEN, CONGRESSIONAL RESEARCH SERVICE, INTRODUCTION TO THE LEGISLATIVE PROCESS IN THE U.S. CONGRESS 1–2 (2018), *available at* https://fas.org/sgp/crs/misc/R42843.pdf (on file with *The University of the Pacific Law Review*) (summarizing the process legislation must go through to become law).

and interested parties publicly discuss the bill's provisions, which would allow the statute to best reflect the realities of privacy and database security.[277]

A Supreme Court ruling would apply a single standing test to all data breach defendants.[278] This could prove harmful for small businesses that may lack resources to take the protective measures instituted by larger companies.[279] Thus, the statute would limit liability for individuals and small business owners.[280] By limiting liability for smaller businesses, the statute would encourage these businesses to guard against data breaches while not being overly burdensome.[281]

In addition to resolving the standing question, the law could address remedies as well.[282] Affected individuals may take protective measures against data breaches, such as freezing their credit or signing up for credit monitoring services.[283] Therefore, affected people may have to spend money to protect against identity theft and fraud.[284] Recognizing these costs, the statute would provide individuals affected by a data breach the opportunity to freeze their credit free of charge with credit bureaus.[285] The business controlling the database, such as Neiman Marcus in the *Remijas* case, would pay for the credit freezes.[286] Thus, the statute would provide a measure of compensation to those impacted by data breaches without resort to the courts.[287]

VI. CONCLUSION

Data breaches are an increasingly common occurrence and can lead to

277. *See id.* at 3–4 (stating committees may hold hearings on bill in which the interested parties may discuss the strengths and weaknesses of the bill).

278. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409, 414 n.5 (2013) (noting the discussion of the "certainly impending" test and "substantial risk" test).

279. *See* Andrew Zaleski, *Congress Addresses Cyberwar on Small Businesses: 14 Million Hacked Over Last 12 Months*, CNBC (Apr. 5, 2017), https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html (on file with *The University of the Pacific Law Review*) (noting small businesses often cannot afford to have IT departments).

280. *Supra* Part V.B.

281. *See supra* Part V.B (proposing a statute which would limit liability for small businesses).

282. *See* Mank, *supra* note 53, at 1365 (stating Congress could pass a law providing better remedies for data breach litigants).

283. Brian Fung, *After the Equifax Breach, Here's How to Freeze Your Credit to Protect Your Identity*, WASH. POST (Sept. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/09/after-the-equifax-breach-heres-how-to-freeze-your-credit-to-protect-your-identity/ (on file with *The University of the Pacific Law Review*).

284. *See* Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (on file with *The University of the Pacific Law Review*) (noting credit monitoring services can cost $30 a month).

285. *Supra* Part V.B; Irby, *supra* note 264.

286. *Supra* Part V.B.

287. *See id.* (proposing a statute under which individuals and businesses controlling databases would pay for credit freezes for affected individuals in the event of a data breach).

consequences, including identity theft and fraud.[288] Like all other plaintiffs, individuals attempting to sue for a data breach in federal court must have suffered an injury sufficient to confer standing.[289] In data breach cases, plaintiffs may try to sue on the basis of the increased risk of identity theft due to identity theft not yet occurring.[290] However, whether this is a sufficient injury may depend on which court hears the lawsuit.[291]

Circuit courts have continued to diverge over whether the future risk of identity theft is sufficient for standing purposes.[292] However, courts finding the future risk sufficient take the better approach because criminals hack databases to sell the stolen personal information or use it to commit other crimes; therefore, the risk of identity theft is not speculative.[293] Thus, the Supreme Court should adopt a rule that the future risk of identity theft or fraud due to a data breach is a sufficient injury for standing.[294]

Alternatively, Congress could resolve the data breach standing issue with a statute.[295] A data breach law would have certain advantages over a Supreme Court decision, such as the flexibility to compensate affected individuals before a lawsuit.[296] With either the Supreme Court issuing a decision or Congress passing a statute, the circuit split would finally end and give certainty to data breach plaintiffs and defendants.[297]

288. *Supra* Part I.

289. *Supra* Part II.

290. *Supra* Part I.

291. *Supra* Part II.

292. *Supra* Part IV.

293. *Supra* Part IV.C.

294. *Id.*

295. *Supra* Part V.

296. *Supra* Part V.C.

297. *See supra* Part II; Part IV (noting how similar data breach plaintiffs may experience different outcomes based on the court).

* * *