Louisiana Law Review

Volume 80
Number 3 *Spring 2020*

Article 11

9-15-2020

Please Hold Your Applause: How Clapper v. Amnesty International USA Deters Data Breach Litigants from Seeking a Judicial Remedy

Harrison M. Martin

Please Hold Your Applause: How *Clapper v. Amnesty International USA* Deters Data Breach Litigants from Seeking a Judicial Remedy

Harrison M. Martin[*]

TABLE OF CONTENTS

∗ I would like to thank Professor John Devlin and the *Louisiana Law Review* Editorial Board for their guidance in writing this Comment. Special thanks to my parents and brothers for their support, Blakeley for her encouragement, and Brian Eno, whose discography fueled my writing process.

INTRODUCTION

In 2017, one of the largest credit monitoring companies in the United States—Equifax[1]—suffered a cybersecurity breach that affected up to 143 million Americans.[2] The Equifax hackers gained access to consumers' names, dates of birth, addresses, and Social Security numbers.[3] From those affected by the data leak, hackers obtained approximately 209,000 consumers' credit card information.[4] Similarly, in October 2017, Yahoo! announced that it had suffered two separate data breaches that affected all three billion of its users.[5] Along with security questions and answers, hackers obtained user information, such as names, email addresses, telephone numbers, dates of birth, and passwords.[6] This sensitive information was eventually bundled and sold on the dark web[7] for approximately $1,800.00[8] per transaction.[9]

---

1. *How to Protect Yourself Against the Theft of Your Identity*, ECONOMIST (Sept. 14, 2017), https://www.economist.com/finance-and-economics/2017/09/14/how-to-protect-yourself-against-the-theft-of-your-identity [https://perma.cc/H9GF-MCZX].

2. Seena Gressin, *The Equifax Data Breach*, FED. TRADE COMM'N, https://www.ftc.gov/equifax-data-breach [https://perma.cc/XT7K-58ZW] (last visited Oct. 10, 2018).

3. *2017 Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/frequently-asked-questions/ [https://perma.cc/9GA5-43EL] (last visited Oct. 10, 2018).

4. *Id.*

5. Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017, 9:23 PM), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 [https://perma.cc/UJ9X-3MNH].

6. *Yahoo Security Notice December 14, 2016*, YAHOO!, https://help.yahoo.com/kb/account/SLN27925.html?guccounter=1 [https://perma.cc/6FBY-AYU6] (last visited Oct. 10, 2018).

7. The dark web is a designated section of the internet. It fundamentally provides a private, anonymous, and heavily encrypted browsing experience. Some (but not all) of the dark web's contents contain illicit material and black-market trade. Mark Ward, *Tor's Most Visited Hidden Sites Host Child Abuse Images*, BRIT. BROADCASTING CO. (Dec. 30, 2014), https://www.bbc.com/news/technology-30637010 [https://perma.cc/FP7C-LWP8].

8. Paul Szoldra, *The Dark Web Marketplace Where You Can Buy 200 Million Yahoo Accounts Is Under Attack*, BUS. INSIDER (Sept. 22, 2016, 2:09 PM), https://www.businessinsider.com/real-deal-market-ddos-2016-9?r=DE&IR=T [https://perma.cc/B2FU-Q7TT].

9. Verizon contemporaneously acquired Yahoo! at the time the data breach became known to the public. Verizon lowered its valuation price by $350 million

Data breaches occur more frequently than ever because of commercial entities' need to store exponentially increasing volumes of digital information.[10] Each year, millions of Americans are left without legal recourse when hostile hackers steal their information.[11] The consequences are notably damaging, harming consumers and businesses alike.[12] Businesses hosting the stolen data can experience substantial lost profits,[13] and vulnerable consumers must often take preventive measures[14] to combat identity theft and other fraudulent misuses.[15]

Consumers seeking recompense from having their data stolen often take their claims to court for damages in a class action lawsuit. In the pleading stages of these victims' lawsuits, however, courts frequently dismiss the cases for lack of Article III standing.[16] Courts reason that obtaining personal data through a breach is too speculative of a future damage to be redressable until fraudulent charges have actually occurred.[17] This rationale is especially problematic for consumers. As stolen

---

in response to the data breach's damaging effect to Yahoo!'s reputation and competence. Kim S. Nash & Ezequiel Minaya, *Due Diligence on Cybersecurity Becomes Bigger Factor in M&A*, WALL ST. J. (Mar. 5, 2018, 12:01 AM), https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061 [https://perma.cc/LPT9-BA5U].

10. Long Cheng, Fang Liu, & Danfeng (Daphne) Yao, *Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions*, WIREs DATA MINING KNOWLEDGE DISCOVERY 1, 2–3 (2017), https://onlinelibrary.wiley.com/doi/pdf/10.1002/widm.1211 [https://perma.cc/H2EB-GUM9].

11. Michael S. Finkelstein, *Overview of Data Breach Litigation in Louisiana: A Look into Its Uncertain Future*, 63 LA. B.J. 106 (2015).

12. Warwick Ashford, *Data Breaches to Affect Future Sales*, COMPUTER WEEKLY (Feb. 8, 2018), https://www.computerweekly.com/news/252434663/Data-breaches-set-to-affect-future-sales [https://perma.cc/P5JB-M5VX].

13. For example, Target Corporation's quarterly earnings dropped 40%, or $441 million, following a public announcement that the company experienced a data breach. *See* Elizabeth A. Harris, *Data Breach Hurts Profits at Target*, THE NEW YORK TIMES, (Feb. 26, 2014), https://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html [https://perma.cc/GE3Y-KHHF].

14. In a global survey of 7,500 consumers, 90% feared that their personal information would be stolen in a future data breach, with identity theft as one of the primary concerns following a breach. *Id*.

15. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017); *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015).

16. U.S. CONST. art. III, § 2 ("The judicial Power shall extend to all Cases . . . [and] to Controversies . . . .").

17. Finkelstein, *supra* note 11.

information is passed from hand to hand, the chain of causation becomes attenuated, thus making it difficult for consumers to connect the court's identified injury—actual misuse of the information—to the breach.[18] Similarly troubling is how hackers make use of the stolen data. Third parties may hold personal information obtained in a data breach for years before committing identity theft.[19] Consequently, once hackers sell stolen data on the internet, fraudulent use of the personal information may continue for years in varying ways.[20]

Contrary to this reasoning, conferring standing for data breach claims is an appropriate outcome that ultimately benefits both consumers and businesses.[21] If courts acknowledge standing for data breach plaintiffs, businesses could be held liable for failing to protect consumer data, thereby causing businesses to heighten their security standards.[22] Businesses, in turn, will have a lower susceptibility of having their cybersecurity compromised, have higher consumer retention rate, and avoid a costly public backlash.[23] These long-term benefits, while costly in the short run, are extremely valuable for preserving profits and mitigating the many expenses associated with a data breach.[24]

---

18. Jennifer Wilt, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases*, 71 SMU L. REV. 615 (2018).

19. To add yet another wrinkle in the standing analysis, in instances where actual fraud takes years to occur, data breach litigants cannot achieve standing because their cases prescribe.

20. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007).

21. JONATHON CLOUGH, PRINCIPLES OF CYBERCRIME 231 (2d ed. 2015) ("While the most obvious impact of identity crime is financial, most of the cost is in fact borne by institutions rather than individuals. In addition to direct financial losses, there are costs associated with reporting, investigating and rectifying instances of identity crime.").

22. Travis LeBlanc, *A Wake-Up Call: Data Breach Standing Is Getting Easier*, 4 CYBERSECURITY LAW REPORT (Jan. 17, 2018), https://www.bsfllp.com/images/content/2/9/v2/2995/2018-01-17-Cyber-Security-Wake-Up-Call-Data-Breach-Standing-Is.pdf [https://perma.cc/RF4H-S52P].

23. See McMillan & Knutson, *supra* note 5, for an example of how costly a data breach can be for a business. Verizon was in the process of acquiring Yahoo! prior to the breach and valued its target company at $4.83 billion. Following the breach, Verizon instead paid $4.48 billion, $350 million less than its initial valuation. *See also* Nash & Minaya, *supra* note 9.

24. Herb Weisbaum, *The Total Cost of a Data Breach – Including Lost Business – Keeps Growing*, NBC NEWS (July 30, 2018), https://www.nbcnews.com/business/consumer/total-cost-data-breach-including-lost-business-keeps-growing-n895826 [https://perma.cc/L57D-DY8R].

This Comment will highlight and attempt to harmonize the disparities among federal courts' standing analyses that arise from data breach litigation. Part I provides background on data breaches and the foundation for standing under Article III of the Constitution. Part II discusses how the United States Supreme Court case *Clapper v. Amnesty International USA* drastically affects the standing analysis for litigants who allege an increased risk of fraud and identity theft following a data breach.[25] Part III highlights the federal circuit split originating from post-*Clapper* data breach standing cases. Part IV identifies the various methods that courts can use to confer standing for data breach litigants and offers statutory reformation and judicial review as potential resolutions for standing in data breach cases. This Comment concludes by urging the Supreme Court to grant a writ of certiorari for a data breach case to provide a uniform standing rule for data breach litigants across the country.

I. OVERVIEW OF DATA BREACHES AND ARTICLE III STANDING

As time's arrow marches forward,[26] businesses small and large grow increasingly dependent on customers' information to maintain growth and profits.[27] In turn, the vast quantities of information that companies store form enlarged targets for hackers.[28] These caches of personal information have become the targets of many hackers looking to exploit weak cybersecurity barriers for their own benefit.[29]

A. Brief Overview of Data Breaches

As society continues to become more internet-dependent, the data stored on computers and cell phones are becoming an increasingly

25. 568 U.S. 398 (2013).

26. *Bojack Horseman: Time's Arrow* (Netflix Sept. 8, 2017).

27. The International Data Corporation forecasts that the Global Datasphere will grow to 175 zettabytes. For reference, one zettabyte is equal to one trillion gigabytes. *See* David Reinsel, John Gantz, & John Rydning, *The Digitization of the World from Edge to Core*, INT'L DATA CORP. (Nov. 2018), https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf [https://perma.cc/KD2T-GAPE].

28. David W. Smith, *Every Company in the World Will Be Hacked in Five Years*, EUREKA (Nov. 8, 2017), https://eureka.eu.com/gdpr/every-company-hacked-within-five-years/ [https://perma.cc/G6G8-9EH3].

29. *Once Stolen, What Do Hackers Do with Your Data?*, SECPLICITY (May 18, 2017), https://www.secplicity.org/2017/05/18/stolen-hackers-data/ [https://perma.cc/8JZM-T4GH].

valuable commodity and ought to be protected as such.[30] Commercial entities have, to an extent, transformed into digital vaults containing masses of sensitive consumer information, including names, dates of birth, Social Security numbers, passwords, email addresses, and more.[31] This sensitive information is valuable not only to businesses and consumers, but also to "black-hat hackers."[32] These nefarious hackers are capable of making sophisticated attacks on businesses' cybersecurity to obtain consumer information.[33] A hacker capable of penetrating a company's consumer database may engage in numerous fraudulent activities,[34] such as identity crimes, credit card skimming, and fraudulent electronic transfer of funds.[35] The distressing possibility of having one's identity stolen in the aftermath of a data breach is concerning.[36] Even more concerning is the fact that breaches in large corporations have cumulated millions of victims at a time.[37] In an instance where hackers compromise personal data through a cybersecurity breach, the consumers may seek a resolution

30. *The World's Most Valuable Resource Is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/96HB-2MRD].

31. Louise Matsakis, *The WIRED Guide to Personal Data (and Who Is Using It)*, WIRED, (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/E69X-7YJQ].

32. Robert Moore, CYBERCRIME: INVESTIGATING HIGH-TECHNOLOGY COMPUTER CRIME, 24 (2d ed. 2011) (describing a black-hat hacker as someone who "violate[s] computer security for little reason beyond maliciousness or for personal gain").

33. CLOUGH, *supra* note 21, at 56.

34. CLOUGH, *supra* note 21, at 216–219.

35. There are numerous potential injuries to consumers who are victims of data breaches. This Comment will focus on the potential for identity theft for the purposes of examining jurisprudence. In the majority of cases, data breach plaintiffs assert future identity theft as the injury-in-fact.

36. *See, e.g.*, Lambert v. Hartman, 517 F.3d 433, 435 (6th Cir. 2008) (wherein a criminal used information on a published traffic citation to obtain a false driver's license and make purchases in the victim's name); *Data Breaches*, IDENTITY THEFT RESOURCE CTR., https://www.idtheftcenter.org/knowledge-base/category/crimidt/ [https://perma.cc/VES2-XYGR] (last visited Oct. 12, 2018).

37. *See In re* Target Corp. Data Sec. Breach Litigation, 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014) ("[O]ver a period of more than three weeks during the 2013 holiday shopping season, computer hackers stole credit- and debit-card information and other personal information for approximately 110 million customers of Target's retail stores.").

through the judicial system, but not without first passing a traditionally broad hurdle: Article III standing.[38]

B. Standing Principles

Standing is a judicially enforced principle that requires a litigant to prove that a justiciable controversy exists in order to appear before a court.[39] In the federal system, the doctrine emanates from Article III of the United States Constitution, which in pertinent part declares, "The Judicial Power shall extend to all Cases . . . [and] to Controversies . . . ."[40] Through a lengthy line of jurisprudence, the Supreme Court molded the "cases and controversies" language of Article III into the standing requirement to promote the separation of powers.[41] The Supreme Court created the standing doctrine to limit its federal judicial power by hearing and deciding only justiciable conflicts.[42]

The Supreme Court determines the existence of standing based on "whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues."[43] The standing requirement mandates three prerequisites a litigant must satisfy: (1) the plaintiff must suffer from a concrete and particularized injury-in-fact that is either actual or imminent; (2) the injury incurred must be fairly traceable to the defendant's actions; and (3) the injury must be redressable by a favorable court decision.[44] The standing analysis prevents abuse of judicial powers by limiting standing to plaintiffs who have been personally injured.[45] Otherwise, lawsuits would flood the federal courts as unaffected third parties seek judicial remedies for any legal issue that they may encounter.[46]

---

38. *See* Fairchild v. Hughes, 258 U.S. 126 (1922).

39. ERWIN CHEMERINSKY, CLOSING THE COURTHOUSE DOOR 96–97 (Yale University Press 2017) (hereinafter "CHEMERINKSY I").

40. U.S. CONST. art. III, § 2.

41. In limiting its ability to only hear cases and controversies, the Supreme Court is prevented from using powers reserved for the executive and legislative branches of government. *See Fairchild*, 258 U.S. 126; Poe v. Ullmann, 367 U.S. 497 (1961); Sierra Club v. Morton, 405 U.S. 727 (1972); Allen v. Wright, 468 U.S. 737 (1984); City of Los Angeles v. Lyons, 461 U.S. 95 (1983); *see also* CHEMERINSKY I, *supra* note 39, at 96.

42. CHEMERINSKY I, *supra* note 39, at 96–97.

43. Warth v. Seldin, 422 U.S. 490, 498 (1975).

44. Ne. Fla. Chapter Associated Gen. Contractors of Am. v. City of Jacksonville, 508 U.S. 656, 663–64 (1993) (citations omitted).

45. CHEMERINSKY I, *supra* note 39, at 96.

46. CHEMERINSKY I, *supra* note 39, at 111.

Litigants often find that the "injury-in-fact" element[47] bars standing.[48] To constitute injury-in-fact, the injury asserted must be "concrete and particularized"[49] and cannot be "conjectural or hypothetical."[50] The actual injury requirement exists for two reasons.[51] First, it incentivizes the plaintiff to litigate for a court-ordered resolution on an adverse issue, as opposed to using the court for a mere advisory opinion.[52] In theory, plaintiffs are discouraged from filing a complaint without an actionable conflict by knowing that their lawsuits would be dismissed in the early stages of litigation, effectively closing the judicial floodgates to frivolous claims.[53] Second, a plaintiff who suffers an injury relies on the court's resolution to right the wrong, creating a "personal stake" in the case's outcome.[54] In essence, requiring such specificity for an injury provides motivation to plead a case and a resolution to a specific conflict.

II. THE EFFECTS OF OVATION—HOW *CLAPPER V. AMNESTY INTERNATIONAL USA* CHANGED THE STANDING ANALYSIS

In contrast to the enduring standing doctrine, data breaches have only recently received attention because of the large scope of cyberattacks and developing efforts to combat them.[55] Lower federal courts remain conflicted about whether the risk of future harm could constitute an injury-in-fact when assessing the legal ramifications of the data breach cases.[56]

---

47. Similar to the injury-in-fact requirement, the second and third elements to standing have complex, varied, and, in some cases, contradictory interpretations that exceed the scope of this Comment.

48. *See, e.g.*, Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) (finding that a damage to occur "soon" is too attenuated to qualify as an injury-in-fact); *see also* City of Los Angeles v. Lyons, 461 U.S. 95 (1983) (finding no injury-in-fact where an injury was uncertain to happen again in the future).

49. *Lujan*, 504 U.S. at 560 (citations omitted).

50. *Id.*

51. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 62 (Wolters Kluwer 5th ed. 2015) (hereinafter "CHEMERINSKY II").

52. *Id.*

53. *Id.*

54. *Id.*

55. *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes*, TRENDMICRO (Aug. 10, 2018), https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101 [https://perma.cc/G9H4-V87T].

56. *See, e.g.*, Reilly v. Ceridian Corp., No. CIV.A. 10-5142 JLL, 2011 WL 735512, (D.N.J. 2011); *see also* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

These early data breach cases have expanded to become the backbone for modern data breach standing analyses.[57]

*A. Pre-*Clapper *Prelude for Data Breach Litigants*

Prior to *Clapper v. Amnesty International USA*, federal courts had differing opinions on Article III standing in data breach cases.[58] *Reilly v. Ceridian Corp.* is a landmark case in which the District Court of New Jersey applied the standing doctrine to the complex nature of data breach litigation.[59] In *Reilly*, the defendant–company suffered a cybersecurity breach that resulted in hackers accessing 27,000 individuals' information, including full names, Social Security numbers, dates of birth, and bank account numbers.[60] In denying the plaintiffs' standing, the court ruled that the plaintiffs failed to allege "any actual or imminent injury-in-fact" simply because the breach had yet to inflict pecuniary damages.[61] Rather than finding the breach itself sufficient to constitute injury to plaintiff, the court narrowly reasoned that because the assailants had not yet misused the information, harm from the breach itself—and thus injury—had not occurred.[62] The Third Circuit Court of Appeals affirmed the district court's decision.[63]

Compare *Reilly* with the Seventh Circuit case *Pisciotta v. Old National Bancorp*, another pioneer in the progression of data breach litigation and the antithesis to *Reilly*.[64] In *Pisciotta*, the plaintiffs submitted an online application to the defendant–company's banking services by inputting their names, addresses, Social Security numbers, driver's license numbers, dates of birth, and credit card information.[65] Following the plaintiffs' applications, the defendant–company fell victim to a "sophisticated, intentional and malicious" cyberattack from a third-party

57. *See, e.g.*, Reilly v. Ceridian Corp., No. CIV.A. 10-5142 JLL, 2011 WL 735512, (D.N.J. 2011); *see also Pisciotta*, 499 F.3d 629.

58. 568 U.S. 398 (2013). *See also* Jane T. Haviland & Kevin M. McGinty, *Supreme Court Declines to Address Circuit Split on Data Breach Standing Issue*, MINTZ (Feb. 28, 2018), https://www.mintz.com/insights-center/viewpoints/2018-02-supreme-court-declines-address-circuit-split-data-breach [https://perma.cc/8ADF-39XY].

59. *Reilly*, 2011 WL 735512 (D.N.J. 2011).

60. *Id.* at *1.

61. *Id.* at *2.

62. *Id.* at *5.

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

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

65. *Id.* at 631.

hacker who stole the customers' personal and financial information.[66] The plaintiffs asserted that they had incurred, and would continue to incur, expenses in their efforts to prevent misuse of their personal and financial information.[67] Similar to *Reilly*, the Seventh Circuit noted that the plaintiffs had not suffered from identity theft at the time of filing, nor did any financial losses occur in their accounts.[68] The *Pisciotta* court, however, disagreed with *Reilly*'s holding that the hackers' failure to yet misuse the information necessarily resulted in denying Article III standing.[69]

Rather, the *Pisciotta* court reasoned that a defendant's action that increases a plaintiff's risk of future harm could satisfy standing's injury-in-fact requirement.[70] According to *Pisciotta*, if the plaintiff faces a greater potential for harm following the defendant–company's failure to protect personal information, the plaintiff has suffered an injury-in-fact sufficient to satisfy the standing requirement.[71] Unfortunately for the litigants, state law prevented the lawsuit from advancing past summary judgment stages,[72] but the *Pisciotta* court's forward-thinking approach to future injuries persisted.

---

66. *Id.*

67. *Id.* at 632.

68. *Id.*

69. "Many of those [data breach] cases have concluded that the federal courts lack jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing. We are not persuaded with the reasoning of these cases." *Id.* at 634 (citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 10 (D.D.C. 2007); Bell v. Acxiom Corp., 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3 2006) (unpublished); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006); Giordano v. Wachovia Sec., LLC., 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) (unpublished)).

70. *Id.*

71. *Id.* at 634, 640.

72. The court acknowledged that the plaintiffs did not come forth with any case or statute from Indiana state law recognizing that the plaintiffs had a theory of recovery. The federal court refused to create a substantive state law for Indiana. *See id.* ("We decline to adopt a 'substantive innovation' in state law . . . or 'to invent what would be a truly novel tort claim' on behalf of the state . . . absent some authority to suggest that the approval of the Supreme Court of Indiana is forthcoming.").

Reilly and *Pisciotta* established the foundation for two divisive interpretations of Article III standing in data breach cases.[73] A court's narrow interpretation of the standing doctrine denies a right of action to a data breach plaintiff: If direct financial injury does not occur following the breach, the plaintiff cannot sufficiently assert injury-in-fact.[74] In contrast, a broad interpretation of the standing doctrine allows a plaintiff to claim substantive future harms as an injury-in-fact.[75] Although these conflicting interpretations of standing seemed polarizing, the 2013 Supreme Court decision of *Clapper v. Amnesty International USA* proved to separate them even further.[76]

B. Clapper v. Amnesty International USA

Clapper v. Amnesty International USA considers temporal issues of future injuries similar to data breach cases and provides a logical framework that substantiates Article III standing for a data breach.[77] The *Clapper* suit arose from a constitutional challenge to the Foreign Intelligence Surveillance Act (FISA),[78] an ordinance that allowed the National Security Agency (NSA) to surveil individuals located outside of the United States.[79] The plaintiffs, primarily composed of attorneys who represented foreign individuals, argued that FISA created an "objectively reasonable likelihood" of injury by intercepting protected attorney–client communications through government surveillance in the future.[80] Further, the plaintiffs argued that FISA forced them to take "costly and burdensome measures" to protect privileged attorney–client information; these measures included ceasing phone and email communications altogether and traveling abroad to have face-to-face conversations.[81] The case hinged

73. *See generally In re* Horizon Healthcare Serv. Inc. Data Breach Litig., 846 F.3d 625 (3rd Cir. 2017); Worix v. MedAssets, Inc., 857 F. Supp. 2d 699 (N.D. Ill. 2012).

74. Reilly v. Ceridian Corp., 664 F.3d 38 (3rd Cir. 2011).

75. *Pisciotta*, 499 F.3d at 634.

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

77. *Id.* Newer Supreme Court cases coexist as precedent for standing, but *Clapper* contains comparable future injury issues and is most commonly cited in data breach cases. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

78. 50 U.S.C. § 1881(a) (2018).

79. *Clapper*, 568 U.S. at 401.

80. *Id.* at 410.

81. *Id.* at 407.

on the injury-in-fact prong of the standing analysis because the NSA had not yet intercepted privileged attorney–client information under FISA.[82]

The *Clapper* plaintiffs experienced difficulty arguing this constitutional claim against FISA for two reasons.[83] First, considering the national security nature of the statute, privileged attorney–client information, and international relations between the United States and foreign citizens in a post-9/11 America,[84] the lawsuit demanded a more scrutinizing standing analysis.[85] Second, the plaintiffs faced an uphill battle in claiming that standing existed by virtue of five imminent, interdependent events.[86]

In a 5–4 decision, the Supreme Court ruled against the plaintiffs, concluding that the future harm alleged was neither imminent nor certainly impending.[87] The Court found that the prior requirement of an "objectively reasonable likelihood" of a future injury did not satisfy standing's "certainly impending" injury-in-fact standard.[88] The Court also addressed the plaintiffs' alleged damages caused by the measures they had taken to avoid FISA-authorized surveillance, such as traveling to foreign territories

82. *Id.* at 406.

83. Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft after* Clapper v. Amnesty International USA, 114 MICH. L. REV. 1471 (2016).

84. *Id.*

85. Raines v. Byrd, 521 U.S. 811, 819–20 (1997) ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional.").

86. *Clapper*, 568 U.S. at 410 (The Supreme Court reasoned that, in order to find an impending threat of future injury, five future actions must occur: "(1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").

87. *Id.* at 414.

88. *Id.* at 410 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)) ("As an initial matter, the Second Circuit's 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury-in-fact.'").

to communicate with their clients.[89] The costs incurred to avoid government monitoring were based on an uncertain fear of surveillance because the government had not yet intercepted privileged attorney–client communications.[90] Any of the plaintiffs' injuries sustained in maintaining privacy, therefore, were self-inflicted and founded on concerns over non-imminent, "hypothetical future harm."[91]

Properly interpreted, *Clapper*'s assertion that a future injury-in-fact must be "certainly impending" did not create a drastically heightened requirement to confer standing onto a plaintiff.[92] Buried within footnote five of *Clapper*'s majority opinion, Justice Alito wrote, "Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about."[93] Additionally, *Clapper* did not overrule prior Supreme Court cases where future harm had not yet occurred, even when their injury-in-fact standards were lower than "certainly impending."[94]

The Court's acknowledgment in *Clapper* that standing did not have to be literally certain has huge implications on constitutional standing: If the future injury-in-fact does not have to be certain, what is the effect of the "certainly impending" language?[95] The phrase is subject to a variety of different interpretations,[96] but two conclusions must be drawn from Justice Alito's assertion.[97] First, a future injury-in-fact does not have to be literally

89. *Id.* at 414.

90. *Id.* at 417.

91. *Id.* at 416 (citations omitted).

92. *Contra* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 364–54 (M.D. Pa. 2015) ("[T]he Supreme Court reiterated that a threatened injury must be 'certainly impending.' This standard establishes a high bar for plaintiffs seeking to recover for injuries which have not in fact occurred, even if they appear likely or probable.").

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

94. *See id.* (citations omitted) ("In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.").

95. *Id.*

96. *Id.* at 432–33 (Breyer, J., dissenting). Prior Supreme Court interpretations of certainty include: reasonable probability; substantially likely; realistic danger; and sufficient likelihood. *See* Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979) ("realistic danger"); Mansanto Co. v. Geertson Seed Farms, 561 U.S. 139, 154–55 (2010) ("reasonable probability"); Pennell v. San Jose, 485 U.S. 1, 8 (1988) ("realistic danger"); Dep't of Commerce v. United States House of Representatives, 525 U.S. 316, 333 (1999) ("substantially likely"); Clinton v. City of New York, 524 U.S. 417, 432 (1998) ("sufficient likelihood of . . . injury").

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

certain to qualify for Article III standing.[98] Second, "substantial risk" of future injury and "certainly impending" risk of future harm are distinct standards, but the "certainly impending" standard does not overrule the "substantial risk" standard.[99]

The Court implicitly reasoned that an "objectively reasonable likelihood" of an imminent damage is a lower threshold for injury-in-fact than "certainly impending." Although the Court did not articulate the difference between "impending" and "imminent," it inferred that the injury must be highly probable under the certainly impending standard.[100] In effect, because of the ambiguity surrounding a heightened standard for injury-in-fact imposed by *Clapper*, confusion continues to afflict the lower courts, particularly for data breach cases. Despite *Clapper*'s statement that "threatened injury must be certainly impending," the Court itself acknowledge that "imminence is concededly a somewhat elastic concept."[101] The Court's admission illustrates how inappropriate it is to rely solely on the temporal confines of a certainly impending injury-in-fact in the context of a data breach.[102] And yet, even after the Supreme Court clarified this standard,[103] federal courts continue to apply the certainly impending standard to assert that data breach victims' injuries are merely speculative and too attenuated to qualify for standing.[104]

III. THE *CLAP*TERMATH

Clapper's aftermath has left lower courts in conflict over the proper standing analysis in data breach cases.[105] Using the facts and the Supreme Court's logic set forth in *Clapper*, some lower courts have found that an increased risk in identity theft and supplemental harms following a data

98. *Id.*

99. *Id.*

100. STEVEN L. EMANUEL, EMANUEL LAW OUTLINES: CONSTITUTIONAL LAW 742 (34th ed. 2016).

101. *Clapper*, 568 U.S. at 432.

102. *Id.*

103. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (citing *Clapper*, 568 U.S. at 414). ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur.").

104. Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 90 (2d Cir. 2017).

105. *See, e.g.*, Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d. 333, 338 ("[T]his Court observed that the Second Circuit had not weighed in on the issue of whether increased risk of identity theft is sufficient for standing in a data breach case . . . . This Court also observed that courts—both circuit and district courts—have split over that issue and reached different results.").

breach does not meet the "certainly impending" standard.[106] Additionally, there is an implicit notion that plaintiffs may rest between the "substantial risk" standard and the heightened "certainly impending" standard and still achieve Article III standing.[107] Because of the ambiguity surrounding *Clapper*, however, it remains unclear what this middle ground is and if this middle ground grants standing to litigants.[108]

Plaintiffs who fail to appropriately connect *Clapper* to their data breach claims as resulting in imminent injury further experience difficulties when a court inappropriately focuses on the failure to sufficiently connect an injury to the initial breach.[109] District and appellate courts often perpetuate the issue by relying on different opinions from sister circuits, causing greater dissonance among varying judicial decisions.[110] Every case contains remarkably similar fact patterns, yet, depending on the jurisdiction, courts reach wildly different outcomes.[111]

Courts that do not confer standing to data breach plaintiffs often narrowly interpret *Clapper*'s "certainly impending" standard. These decisions deter plaintiffs from seeking a judicial resolution for injuries from data breaches, such as increased risk of identity theft and lost time and money.[112] Federal courts that do not find standing for data breach

106. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3rd Cir. 2011). ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of Appellants by making unauthorized transactions in Appellants' names. Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.").

107. *See* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524 (2016) ("Acknowledging that *Clapper* requires a 'certainly impending' future injury, or at least a 'substantial risk' of injury . . . .").

108. *Id.*

109. *See id.* at 532. ("Khan's allegations fall short. Unlike in *Krottner* or *Remijas*, Khan alleges no facts indicating that the hackers have attempted to engage in any misuse of CNHS patients' personal information since the breach was discovered. She alleges no suspicious activity: no unauthorized bank accounts or credit cards, no medical fraud or identity theft, and no targeted solicitations for health care products or services.").

110. *See, e.g.*, *id.* (citing *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 363, 366 (M.D. Pa. 2015); *In re* SuperValu, Inc., 2016 WL 81792, at *5 (D. Minn. 2016).

111. *Compare Khan*, 188 F. Supp. 3d 524, *with Storm*, 90 F. Supp. 3d 359.

112. Michael R. Pennington, *Two More Circuits Find Data Breach Standing Without Proof that Plaintiffs' Data Was Misused*, DECLASSIFIED (Apr. 24, 2018),

litigants dismiss the cases because, despite hackers' unauthorized access and theft of plaintiffs' information, no fraudulent activity actually occurred.[113] For example, one court ruled that the risk of future fraud was "too attenuated" from the initial breach.[114] Often in data breach cases, however, the fraudulent use of the data does not occur until months, or even years, after the initial breach.[115] Thus, no justiciable controversy exists, despite obvious damages—including expenses for precautionary measures, lost time, lost credit rewards, and reduced credit scores—that impact millions of people at a time.[116]

A. Data Breach Cases Confined to Narrow Interpretations of Clapper

Khan v. Children's National Health Systems is a data breach case where the United States District Court of Maryland narrowly read *Clapper* to reject standing.[117] In *Khan*, the defendant–hospital fell victim to an email phishing scheme[118] that allowed hackers to access employees' email accounts and content.[119] The acquired information included patients' personally identifiable information, such as names, addresses, dates of birth, and email addresses.[120] For some victims, the email contents also included medical diagnoses, treatment records, and health insurance information.[121] In response to the data breach, the hospital notified 18,000

---

https://www.classactiondeclassified.com/2018/04/two-circuits-find-data-breach-standing-without-proof-plaintiffs-data-misused/ [https://perma.cc/S8M5-6R6E].

113. *See, e.g.*, *Storm*, 90 F. Supp. 3d. 359.

114. *See, e.g.*, Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89, 90 (2d Cir. 2017).

115. The lapse in time between the breach and actual misuse of information may be extended to the point where the claim may be prescribed. *Supra* note 19. *See also In re* Zappos.com, Inc., 108 F. Supp. 3d 949 (D. Nev. 2015).

116. *See* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 386 (6th Cir. 2016).

117. 188 F. Supp. 3d 524 (D. Md. 2016).

118. "'Phishing'. . . may broadly be defined as 'the creation and use by criminals of emails and websites . . . in an attempt to gather personal, financial and sensitive information.'" CLOUGH, *supra* note 21 at 220 (quoting Binational Working Group on Cross-Border Mass Marketing Fraud, *Report on Phishing: A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States* (2006)).

119. *Khan*, 188 F. Supp. 3d 524.

120. *Id.* at 527.

121. The information obtained did not include medical records or patient charts but did contain "private health care information." *Id*.

patients that their personal information had been stolen, and the patients promptly filed suit.[122]

The named *Khan* plaintiff in the class-action lawsuit alleged an imminent threat of identity theft as a future injury, and she alleged out-of-pocket costs incurred to defend herself against identity and credit theft as actual injuries.[123] The court iterated that, although an unknown third party had compromised the plaintiff's personal information, she failed to allege actual misuse of such information.[124] The court considered whether the hackers intended to obtain the patient data and challenged the hackers' ability to actually misuse the information.[125] Additionally, the court asserted that if the hackers obtained information as an unintended byproduct from a cyberattack,[126] the future risk of fraud or identity theft is not certain.[127] Under the *Khan* analysis, a data breach litigant who does not assert actual misuse of the hacked information does not meet *Clapper*'s "certainly impending" standard of injury-in-fact.[128]

Similar to *Khan*, data breach victims in *Storm v. Paytime, Inc.*, filed a class-action suit in the Middle District of Pennsylvania against the defendant–company for failing to protect sensitive information in a cybersecurity breach.[129] To carry out its contracted services with the plaintiffs,[130] the defendant–company possessed the plaintiffs' full legal

122. *Id*.

123. *Id*. at 527, 529.

124. The court specifically listed examples that could have qualified as misuse. These examples included unauthorized access to bank accounts or credit cards, medical fraud, identity theft, and targeted solicitations for health care products or services. *Id*. at 532.

125. *Id*. at 532–33 ("Thus, the allegations are more akin to those in *Reilly*, where the hackers 'potentially gained access to personal and financial information,' but it was unclear 'whether the hacker read, copied or understood' the plaintiffs' personal data, and there was no indication of misuse.").

126. The court reasoned that, rather than obtaining the patient information, the cyberattack was only intended to gain access to the hospital employees' email accounts. This line of logic problematically failed to address the possibility that the hospital employees' email accounts were targeted for the high likelihood of containing sensitive patient information. *Khan*, 188 F. Supp. 3d at 532–33.

127. *Khan*, 188 F. Supp. 3d at 534 ("[T]here [was] no indication that the patients' personal data was actually viewed, accessed, or copied, or was even the target of the phishing scheme.").

128. *Id.*

129. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 363 (M.D. Pa. 2015).

130. The defendant–company offered services to the plaintiffs' employer, such as payroll services, human resource management, and hourly wage submission. *Id*.

names, addresses, bank account data, Social Security numbers, and dates of birth.[131] The defendant–company suffered a security breach by unknown hackers who gained access to the 233,000 victims' personal and financial information.[132] In an attempt to avoid standing issues resulting from future harm, the plaintiffs alleged both actual damages and an increased risk of identity theft.[133]

The *Storm* court noted that the plaintiffs did not actually suffer identity theft, nor did they allege that the hackers actually misused their personal information in a way that caused pecuniary damages.[134] Primarily influenced by *Reilly*, the court found that the plaintiffs lacked standing for failing to allege an actual injury stemming from a heightened risk of identity theft.[135] Indeed, the *Storm* court narrowly interpreted *Clapper*'s "certainly impending" standard, reasoning that because actual misuse of the data had not occurred after the data breach, identity theft was not imminent.[136] When faced with the claims for out-of-pocket expenses, the court concluded that the costs incurred were manufactured and prophylactic to mitigate an injury that had yet to occur in the same vein as *Clapper*.[137] Thus, the *Storm* plaintiffs lacked standing.[138]

B. Broad Interpretations of Clapper *in Data Breach Cases*

In contrast to the restrictive interpretations found in *Khan* and *Storm*, a growing number of courts have interpreted *Clapper* in a way that confers standing for future injuries.[139] These opinions primarily differ through

---

131. *Id*.

132. *Id*.

133. Plaintiff Wilkinson, a member of the class action lawsuit, alleged actual damages in conjunction with a heightened risk of identity theft from the data breach. Wilkinson's employer suspended his security clearance upon notification that a third party compromised his information. The employer relocated him to a different job site, extending his commute to work by four hours. Wilkinson alleged lost time and travel expenses as actual injuries from the data breach. *Id*.

134. *Id*. at 366 ("[The plaintiffs] have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts.").

135. *Id*. (citing Reilly v. Ceridian Corp., 2011 WL 735512 (D.N.J. 2011)).

136. *Storm*, 90 F. Supp. 3d at 365.

137. *Id*. at 363 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013)).

138. *Id.* at 368–69.

139. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); *In re* Adobe Systems, Inc. Privacy Litigation, 66 F. Supp. 3d. 1197

application of a broader analysis that confers standing onto data breach litigants and do not necessarily rely on any subsequent concrete injury that arises following the breach.[140] Instead, the opinions assign the litigants' original harm as injury-in-fact to the data breach claims and rationalize that impending damages are substantially likely to occur following a breach.[141]

Remijas v. Neiman Marcus Group is such a case, wherein the defendant–company fell prey to a cybersecurity breach upon discovering malware[142] installed on its computer systems.[143] The hackers received access to 350,000 credit cards and fraudulently used 9,200 of them.[144] The plaintiffs easily satisfied the Seventh Circuit's injury-in-fact prong of the standing inquiry because a sizeable portion of the customers had already suffered from fraudulent charges.[145]

Remijas was a fairly noncontroversial case because an actual misuse of the stolen information occurred.[146] The court, however, went a step further and confronted *Clapper*'s "certainly impending" language for data breach victims who had not yet suffered fraudulent charges.[147] Rather than identifying an impending fraudulent activity as the plaintiffs' injury-in-fact, the court determined that the act of stealing the information was itself

(N.D. Cal. 2014); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 386 (6th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

140. *See, e.g.*, *Lewert*, 819 F.3d 963; In re *Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d. 1197; *Remijas*, 794 F.3d 688; *Galaria*, 663 Fed. App'x at 386; *Krottner*, 628 F.3d 1139.

141. *Remijas*, 794 F.3d at 693.

142. Malware, or "malicious software," is a blanket term that describes any malicious program or code that is harmful to systems. *Cybersecurity Basics*, MALWAREBYTES, https://www.malwarebytes.com/malware/ [https://perma.cc/SKD3-772P] (last visited Apr. 1, 2019).

143. *Remijas*, 794 F.3d at 690.

144. *Id*. at 692

145. *Id*.

146. Unlike many data breach cases, some of the *Remijas* plaintiffs had already suffered actual injury from fraudulent charges, so they did not have to heavily rely on the more difficult assertion of an increased risk of identity theft. *Id.*

147. *Id*. at 693 ("What about the class members who contend that unreimbursed fraudulent charges and identity theft may happen in the future, and that these injuries are likely enough that immediate preventive measures are necessary?").

the beginning of the litigants' injury.[148] The court stated that the plaintiffs "should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing" because it was likely that such an injury would occur following a data breach.[149] In a provocative conclusion to the injury-in-fact prong of its standing inquiry, the court posited, "Why else 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."[150] The Seventh Circuit's straightforward reasoning makes common and logical sense.[151] In most data breaches, hackers deploy technically complex, time-intensive mechanisms to penetrate a company's cybersecurity infrastructure and gain access to the consumers' protected information.[152] The hackers will either misuse this valuable information themselves or distribute it to other individuals who have an interest in misusing the information.[153] As the Seventh Circuit noted, no alternative rationale exists for a black-hat hacker to breach a business's cybersecurity and steal consumer data. The security breach is thus merely the means to the black-hat hackers' ultimate objective: using the protected information.[154]

Critics of the *Remijas* decision have challenged its jurisprudential value as inconsequential for data breach plaintiffs who have yet to

148. *Id* at 693. ("[I]n our case, there is no need to speculate as to whether [the Neiman Marcus customers'] information has been stolen and what information was taken.").

149. *Id*.

150. *Id*.

151. *See id.*

152. *Id*.

153. *Id*.

154. There are alternate explanations for why a hacker would breach a company's implemented cybersecurity. For example, "white-hat hackers," or "ethical hackers," are individuals who penetrate cybersecurity barriers to expose flaws that black-hat hackers could exploit in a future attack. White-hat hackers typically report this information for the purposes of improving the company's cybersecurity. The data breaches referenced above were all unauthorized and carried out by black-hat hackers. Mark Ward, *Sabotage in Cyberspace – The Threat to National Security from Computer "Terrorists" Are after Nothing More than an Intellectual Thrill*, NEWSCIENTIST (Sept. 14, 1996), https://www.newscientist.com/article/mg15120471-700-sabotage-in-cyberspace-the-threat-to-national-security-from-computer-terrorists-is-vastly-overblown-most-hackers-are-after-nothing-more-than-an-intellectual-thrill/ [https://perma.cc/YM3R-3U3B] (last visited Nov. 11, 2018).

experience actual misuse of their information.[155] Nevertheless, the influence of *Remijas*'s expansion of the standing analysis can be seen in the more recent case, *Galaria v. Nationwide Mutual Insurance Co*.[156] *Galaria* demonstrates a broad application of *Clapper* within a data breach case where hackers gained unauthorized access to 1.1 million customers' personal information.[157]

In *Galaria*, the Ninth Circuit found that when hackers intentionally breach a company's cybersecurity to steal customer data, it is reasonable to assume that the hackers will commit further harms with the consumers' information.[158] The court reasoned that data breach victims need not speculate about whether future injury would occur because the injury had already occurred: Ill-intentioned hackers stole their information.[159] Furthermore, the court noted that, following a data breach, expending time and money to combat misuse of stolen information is not a manufactured injury but, rather, a concrete injury imposed on the victim to prevent an imminent harm.[160] The *Galaria* court bolstered the *Remijas* court's opinion by conferring standing onto data breach litigants who had their sensitive information stolen but not yet misused.[161] Appropriately, the court considered the breach and the resulting theft of information to constitute an injury in itself.[162] In turn, this understanding dismantles the narrow interpretation of *Clapper* for data breach cases, which relies on the actual occurrence of fraud or identity theft following the information theft.[163] The *Galaria* court's methods of finding an injury-in-fact may be used as a foundation for future data breach litigants to plead their cases.

---

155. For example, the *Khan* court dismissed the *Remijas* court's logic by asserting that the group of plaintiffs who suffered from actual misuse influenced the court's standing decision for the group that had not yet suffered from misuse. *See Khan*, 188 F. Supp. 3d 524, 532 (D. Md. 2016) (Unlike in *Remijas*, "Khan alleges no facts indicating that the hackers have attempted to engage in any misuse of CNHS patients' personal information since the breach was discovered.").

156. 663 Fed. App'x 384, 386 (6th Cir. 2016).

157. The information compromised included names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers. *Id*.

158. *Id*. at 388 ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.").

159. *Id*.

160. *Id*. (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013)).

161. *See id.*

162. *Id*.

163. *Id*.

IV. AVAILABLE APPROACHES TO CONFER STANDING TO DATA BREACH LITIGANTS

Courts that do not confer standing to data breach plaintiffs often reason that actual misuse of the stolen information has yet to occur.[164] This rationale relies far too heavily on *Clapper*'s "certainly impending" standard and does not consider why standing must be conferred onto the plaintiffs in the first place. Requiring an injury-in-fact ensures that the plaintiff has a stake in the litigation's outcome.[165] Data breach plaintiffs are not frivolously filing lawsuits to make a quick dollar. Rather, they are seeking indemnification from companies that are thought to have negligently mishandled consumers' private information. Although this sentiment alone is undoubtedly insufficient to win an entire case, showing that an injury has occurred through the breach itself should be adequate to surpass the low threshold for standing. Under this foundation, a data breach plaintiff could, at the very least, continue into the pretrial litigation stage of her claim. Moreover, the defendant–company would still have ample opportunity to defeat the case in the many other pretrial stages or on the merits.

Arguably, the origin of the injury should be the moment a hacker compromises a company's cybersecurity and obtains the consumers' private information, provided that the company implements insufficient cybersecurity measures. Data breach victims suffer an injury by having their information stolen. Victims suffer a continuing harm by having their information leaked and through the degradation of their data's value through an economic loss principle.[166] Accordingly, United States data breach laws should be altered to implement the data breach itself as

---

164. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017) (finding that potential misuse of sensitive personal information is not sufficient to establish a substantial risk of harm).

165. CHEMERINSKY II, *supra* note 51, at 62.

166. "Economic loss" is pecuniary damage not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property. Ordinarily, there is no liability in tort for economic loss caused by negligence in the performance or negotiation of a contract between the parties. In some instances, however, a defendant may be liable for pure economic loss. The Third Restatement of Torts provides:

> One who, in the course of his business, profession, or employment, or in any other transaction in which he has a pecuniary interest, performs a service for the benefit of others, is subject to liability for pecuniary loss caused to them by their reliance upon the service, if he fails to exercise reasonable care in performing it.

RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM, §§1, 3.

satisfying the injury-in-fact requirement for victims to have access to the justice system.

Before a legal reconciliation among the circuits can occur, data breach litigants must be able to sufficiently identify the varying methods of establishing an injury-in-fact. Adequately pled data breach cases sufficient for Article III standing may include emphasizing the costs incurred to mitigate the leak of personal information, identifying the breach itself as the initial point of injury, and analogizing Supreme Court jurisprudence that contains legally comparable principles.

A. Data Breach Standing—More Ways than One

Pecuniary damages are the easiest way for a data breach victim to show that an injury-in-fact occurred.[167] In most data breach cases, plaintiffs incur concrete and tangible expenses for credit monitoring services.[168] In instances where courts do not confer standing on data breach plaintiffs, the courts address credit monitoring expenses through the lens of *Clapper*.[169] *In re Zappos.com, Inc.*, for example, determined that the costs incurred to prevent identity theft and fraud were not enough to confer standing because the future threat of identity theft was neither imminent nor immediate.[170] Contrary to *Clapper*'s pertinent facts, data breach plaintiffs are not, in fact, inflicting harm on themselves from fear of a hypothetical future harm.[171] Rather, the harm is present once the hackers steal customers' sensitive information.[172] The imminent harm of identity theft is substantively elevated beyond speculation when consumers' personal information is stolen.[173] Any pecuniary expenses incurred to mitigate the future risk of identity theft, therefore, cannot be classified as manufactured standing from a hypothetical harm.[174]

---

167. *See* Spokeo, Inc., v. Robins, 136 S. Ct. 1540, 1548 (2016) ("A 'concrete' injury must be '*de facto*;' that is, it must actually exist. When we have used the adjective 'concrete,' we have meant to convey the usual meaning of the term—'real,' and not 'abstract.'") (citations omitted).

168. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); *Beck*, 848 F.3d at 268; *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015).

169. *See, e.g.*, In re *Zappos.com, Inc.*, 108 F. Supp. 3d at 953.

170. *Id.* (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 415 (2013)).

171. *Clapper*, 568 U.S. at 416.

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

173. *Id*.

174. *Id*.; *see also* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016). The Seventh Circuit reasoned that an increased risk of fraudulent

Even if the victims do not experience actual fraud, they must refrain from using their credit cards, miss opportunities to build credit rewards, and refrain from making purchases when transitioning cards or credit services.[175] The inability to use a credit card may be seen as only a minor inconvenience to some, but it should suffice to meet the low bar of injury-in-fact for Article III standing.[176] Similarly, the time expended receiving new government documents, such as a Social Security number or driver's license, is material. Courts have found the value of time expended to mitigate future identity theft to qualify as an injury-in-fact, even in an instance in which it took only three days to unfreeze a plaintiff's credit account.[177]

These varying methods of conferring standing on a data breach plaintiff absent a direct pecuniary loss are plausible, especially in light of Supreme Court jurisprudence. For example, compare a typical data breach with the Supreme Court case *Davis v. Federal Election Commission*.[178] In *Davis*, the plaintiff, a House of Representatives candidate, sued over a law that allowed his opponent to receive a disproportionate amount of campaign contributions in an uncharacteristically beneficial way.[179] Both parties agreed that the opponent had not yet exploited the statute to receive an unfairly higher amount of campaign contributions.[180] Nonetheless, the Supreme Court conferred standing because the plaintiff, at the time of filing the lawsuit, faced a "realistic and impending threat of direct injury" that his political opponent would take advantage of the statute.[181] The facts presented under the *Davis* case can be easily analogized to the facts that a data breach litigant would assert.[182] In the context of a data breach case, a hacker obtaining consumer information is comparable to the statute at issue in *Davis*, which merely granted the capability of exploitation.[183] Even if data breach hackers have not yet misused the information at the moment of the data breach, they have gained the capability to cause an impending threat of direct injury, constituting an injury-in-fact.[184]

---

charges and identity theft were concrete enough to support a lawsuit because "their data ha[d] already been stolen." *Id.* at 967.

175. CHEMERINSKY I, *supra* note 39, at 101.

176. *Id*.

177. Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 829 (7th Cir. 2018).

178. Davis v. Federal Election Comm'n, 554 U.S. 724, 728 (2008).

179. *Id*. at 735.

180. *Id*.

181. *Id*.

182. *Id.* at 728.

183. *Id*.

184. *Id*.

Similarly, Davis's political opponent had not yet exploited the statute, but the court conferred standing because the statute granted the capability of exploitation.[185]

Although plaintiffs can show that injuries have occurred in many ways following a data breach, if Congress or the Supreme Court does not streamline the litigation process on a national level, different federal circuits will likely continue to produce contradictory rulings on the issue. In understanding how data breach litigants may currently structure their pleadings to sufficiently support injuries-in-fact on an individual level, it is worth examining how data breach litigation can be restructured on a national level to avoid the standing issue altogether.

B. Standing Salvation Through Statutory Reformation

Congress should consider enacting a data breach statute that protects consumer interests by granting a private right of action. The statute would ideally qualify a data breach as a redressable injury, leaving no room for ambivalence in a court's standing analysis. *Spokeo v. Robins*, a recent Supreme Court case, speaks to the effectiveness of private rights afforded under statutory provisions that could be applied to a data breach.[186] In *Spokeo*, the plaintiff filed suit against the defendant–company for allegedly violating the Federal Credit Reporting Act (FCRA)[187] by publicizing inaccurate personal information.[188] The Court spent most of its discussion determining whether a mere procedural violation of a statute was sufficient to establish injury-in-fact in the absence of tangible, concrete injuries.[189] The majority opinion held that, although some cases have held that the procedural violation of a statute satisfies the injury-in-fact requirement, standing cannot be achieved where the statutory violation did not result in harm.[190] The Court reasoned that the defendant–company could not have injured the plaintiff simply by disseminating inaccurate personal information, even if such dissemination violated a procedural statute.[191]

185. *Id*.
186. Spokeo, Inc., v. Robins, 136 S. Ct. 1540 (2016).
187. 15 U.S.C. § 1681e(b), the statute at issue in *Spokeo*, requires consumer reporting agencies to "follow reasonable procedures to assure maximum possible accuracy" of consumer reports. *Spokeo*, 136 S. Ct. at 1543.
188. *Spokeo*, 136 S. Ct. at 1548–50.
189. *Id*. at 1545.
190. *Id*. at 1550.
191. *Id*.

Justice Thomas's concurrence made a critical distinction between procedural statutes that govern public rights and private rights.[192] According to Justice Thomas, public rights created through federal legislation often raise standing issues when challenged because the litigant effectively argues that a public executive agency is not acting in accordance with the law.[193] In this instance, the executive agency is not necessarily harming the individual directly because the agency's procedural violation is likely insufficient to qualify as a substantive injury.[194] In contrast, statutorily created private rights allow a litigant to assert that another private party violated her individual rights.[195] The majority opinion references these private rights as the type that may constitute an injury in itself.[196] If a defendant violates a duty owed to an individual, therefore, the statutory violation constitutes a harm in itself and does not raise the same standing issues as a public right.[197]

In light of *Spokeo*, Congress should enact a federal data breach statute that allows for uniform application throughout the country, preempting current state data breach legislation.[198] Each state has its respective data breach notification statute that requires businesses to timely notify consumers when security threats compromise the businesses' information.[199] Every statute contains similar provisions but varying verbiage and legal ramifications.[200] Generally, these data breach notification statutes contain provisions that provide: (1) what constitutes a data breach; (2) who must comply with the law; (3) a definition of "personal information"; and (4) an imposition of responsibility upon businesses to notify consumers when hackers compromise their cybersecurity.[201] Despite in-depth definitions and clear efforts to protect consumers' information in a data breach, not a single piece of state

192. *Id*. at 1553 (Thomas, J., concurring).

193. *Id*. at 1552.

194. In matters regarding procedural violations, the plaintiff must show a nexus between the procedural violation and a substantive injury therefrom. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

195. *Spokeo*, 136 S. Ct. at 1553 (Thomas, J., concurring).

196. *Id*. at 1552 (Thomas, J., concurring).

197. *Id*. at 1554.

198. *See generally id.* (majority opinion); *see also Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/TY5M-P2HV].

199. *Security Breach Notification Laws*, *supra* note 198.

200. *Id*.

201. *Id*.

legislation grants a private right of action to the consumers against the company for negligently handling their private information.[202] A federally enacted data breach protection law would ultimately promote uniformity in how companies handle data breaches, alleviate complicated jurisdictional issues,[203] and, most importantly, provide a private right of action for consumers injured in a data breach.[204] This right of action would effectively hold companies responsible for negligently mishandling consumer data and bypass standing issues by making the source of injury stem from the violation of the statute itself.[205]

In drafting the data breach statute, Congress could draw inspiration from the European Union's recently enacted General Data Protection Regulation (GDPR).[206] The GDPR is immensely broad in scope and encompasses a multitude of rights regarding personal information and data.[207] In summary, the GDPR mandates fundamental rights to protect consumers' personal data once the data is under another organization's control.[208] Should an individual provide personal information to a business, the business is responsible for safeguarding consumer data against third parties and is liable for any misuse of data beyond the consumer's consent. Any violation of the GDPR, including "material and non-material damage" resulting from the violation of a company's responsibility to protect consumer data, can result in the right to receive compensation for the injury.[209] The legislation notes that "[t]he concept of damage *should be broadly interpreted* in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of [the] Regulation."[210] A congressionally enacted statute that draws influence

202. Data breach notification laws typically allow civil recovery of damages when a business fails to notify consumers of a data breach, but not for the damages accrued from the breach itself. *See, e.g.*, LA. REV. STAT. § 51:3075 (2018).

203. Courtney M. Bowen, *Data Breach 101, Part I: Data Breach Notification Laws*, PROSKAUER (Mar. 16, 2017), https://www.mindingyourbusinesslitigation.com/2017/03/data-breach-101-part-i-data-breach-notification-laws/ [https://perma.cc/922Z-4URX].

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

205. *Id*.

206. Parliament and Council Regulation 2016/679 of May 4, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

207. *See generally id*.

208. *See generally id*.

209. *Id*.

210. *Id.* (emphasis added).

from the GDPR could serve multiple benefits.[211] First, the statute would provide access to the justice system for data breach litigants by establishing that the failure to safeguard data is, in fact, a sufficient injury for Article III standing.[212] Second, the statute would incentivize companies to strengthen their cybersecurity measures to avoid costly litigation expenses and potential penalties from the government.[213] As a result, the statute would better protect consumers' information, thwart hackers' attempts to misuse information, and maintain where consumer information belongs—the consumers.[214]

As appealing as a national data breach protection statute may be, passing a statute that puts large corporations at risk for liability will likely be extremely difficult given Congress's current partisan state.[215] In a case of congressional standstill, one more viable alternative remains.

C. Judicial Review for Data Breach Litigation

Considering that Article III standing is a judicially enforced concept, it is rational for the Supreme Court to dictate whether a data breach would constitute an injury-in-fact under the standing doctrine.[216] Accordingly, a sensible resolution to the data breach standing conflict involves the Supreme Court granting a writ of certiorari for a pending data breach case.[217]

Granting a writ for a data breach case allows the Court to address the multiple legal issues that specifically cloud data breach litigation: (1) the

---

211. *See generally id*.

212. *Id*.

213. James McGrath, *2.1 Million Reasons to Toughen Up on Data Security*, MYOP (Feb. 8, 2018), https://www.myob.com/au/blog/penalties-for-data-security-breaches/ [https://perma.cc/7ST7-8MPT].

214. *See generally* GDPR, *supra* note 206.

215. Personal data protection bills have been proposed in the past, but none have successfully passed. *See, e.g.*, Data Security and Breach Notification Act of 2015, S. 177, 106th Cong. (2015).

216. Lexmark Int'l, Inc., v. Static Control Components, Inc., 572 U.S. 118, 125 (2014) ("From Article III's limitation of the judicial power to resolving 'Cases' and 'Controversies,' and the separation-of-powers principles underlying that limitation, the Supreme Court has deduced a set of requirements that together make up the irreducible constitutional minimum of standing.").

217. A writ of certiorari orders a lower court to deliver its records from a case so that a higher court may review them. It is the vehicle that allows a higher court to hear and rule on a lower court opinion. *Writ of certiorari*, LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/wex/writ_of_certiorari [https://perma.cc/D3WJ-RPUX] (last visited Apr. 1, 2019).

temporal aspect of future harm from stolen information; (2) whether the breach itself constitutes an injury or if the personal data must be misused; and (3) whether the hacked data equates to some form of loss.[218] Likewise, a Supreme Court decision would resolve the standing doctrine circuit split that plagues the lower courts.[219] Ideally, the Supreme Court would rule that a data breach qualifies as an injury-in-fact, particularly without a tangible instance of theft. Under this ruling, a data breach plaintiff would have an opportunity to plead her case before the court beyond the summary judgment stage of litigation.

V. CONCLUSION

Data breach litigation has divided circuits across the country, largely because of complications from applying the murky, contradictory language of *Clapper v. Amnesty International USA* and data breach cases.[220] Upon examining *Clapper*'s language and analyzing the underlying principles that construct Article III standing, courts should confer standing on data breach litigants. Judicial opinions that focus too much on the attenuated circumstances of imminent fraud or identity theft misconstrue the very reasons why standing is necessary at all. The fundamental principles of standing ensure that litigants are enforcing their own individual rights, not the rights of others, and that each plaintiff is legitimately seeking a judicial resolution, as opposed to a court-ordered form of legal advice.[221]

Data breach litigants suffer an injury through the theft of their personal information.[222] The theft itself should be analyzed by the court as the beginning of the plaintiff's injury-in-fact, rather than the reasonably foreseeable end result of fraud or identity theft.[223] In addition to the act of the breach itself, courts should confer standing on data breach litigants for supplemental injuries, including emotional injury, lost time, and mitigating circumstances. Under this framework, each data breach

218. Financial and cybersecurity analysts have established that a data breach can result in economic loss for the company. However, courts have yet to address whether an economic loss results from the value of the consumers' data. *See, e.g.*, Herb Weisbaum, *supra* note 24; *see also* McMillan & Knutson, *supra* note 5.

219. *Resolving Circuit Splits*, LEGAL INFORMATION INST., https://www.law.cornell.edu/supct/cert/supreme_court_2014-2015_term_highlights/part_one/resolving_circuit_splits [https://perma.cc/P526-87ZU] (last visited Jan. 22, 2019).

220. *See* discussion *supra* Section II.B.

221. *See* discussion *supra* Section I.B.

222. *See* discussion *supra* Section IV.A.

223. *Id*.

plaintiff would be able to have her day in court, as opposed to being denied in the early standing stage of pretrial litigation. Likewise, where the plaintiff fails to assert a sufficient injury beyond the motion to dismiss stages, the court will be able to rule in favor of the defendant after weighing the pertinent facts of the case.

To resolve the tensions that arise when courts analyze standing for data breach cases, Congress should enact federal legislation that provides a private right of action to consumers who suffer a data breach.[224] Once a business fails to protect consumer data, it will be in violation of a private right of action, which, in turn, will undoubtedly become a justiciable controversy under the standing doctrine. In the likely case of a congressional standstill, the Supreme Court should grant a writ of certiorari for a data breach case on appeal.[225] Through judicial review, the Supreme Court would be the most capable body to resolve the future injury issues that arise from its *Clapper* ruling and could award damages to the consumers at the businesses' expense. By hearing such a case and implementing a jurisprudential rule, the Court could further reinforce the traditional principles of the standing doctrine in a new era dominated by advanced uses of cybertechnology.

224. *See* discussion *supra* Section IV.B.
225. *See* discussion *supra* Section IV.C.