LEAVING CLASS ACTION PLAINTIFFS WITH TOO MANY LEGS TO STAND ON: THE INCONSISTENT APPLICATION OF ARTICLE III STANDING REQUIREMENTS IN DATA BREACH CASES

CHRISTINA BEHAN*

I. INTRODUCTION 169
II. THE COMMON LAW DEVELOPMENT OF ARTICLE III STANDING 171
A. The Troublesome "Injury in Fact" Element 173
III. THE CIRCUIT SPLIT 174
A. Standing Based on Increased Risk of Identity Theft 175
B. Increased Risk of Identity Theft is Insufficient to Meet the Standing Requirements 177
C. The Negative Impact of the Circuit Split 180
IV. THE SUPREME COURT'S PRECEDENT ON "INJURY IN FACT" REQUIREMENTS 182
A. Analysis of the Cases and the Stance the Supreme Courts Would Likely Take on the Circuit Split 184
1. Analysis of the Sixth, Seventh, Ninth, and D.C. Circuits 184
2. Analysis of the Third, Fourth, and Eighth Circuits 188
V. PROPOSED "INJURY IN FACT" STANDARD TO RECTIFY THE CIRCUIT SPILT 189
A. Policy Considerations for the Statutory Proposed Standard 192
B. Impact the Proposed Balancing Test Will Have on the Federal Courts 194
VI. CONCLUSION 195

I. INTRODUCTION

While technological innovations over the past 30 years have made life more efficient and comfortable, those advances come at a price. Private information is now exceedingly easier to obtain without the individual's knowledge or consent. In today's digital age of online banking, quick-pay by using a phone, and automatic deposits of paychecks, large amounts of personal information are stored on online databases. Although these technological advances make life easier, they put individuals' information at risk to be misused by criminals. Online hackers make it their job to breach servers carrying personal information, presumably to misuse that information for their own personal gain.[1] The companies or agencies entrusted with storing this private information have a responsibility to keep that information secure,[2] but this can be challenging when highly motivated hackers work around the clock to breach those servers.

---

* Florida State University College of Law, J.D. Candidate, 2019. Special thanks to Professor David Landau for guidance throughout the note-writing process. I also thank my mom and grandma, Mary Behan and Felicia Chiapparelli, for all their love and support.

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

2. Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B.J. 30, 34 (2016).

As the CEO of Yahoo put it, "[w]hat is clear is that users own their data and should have control of how their data is used."[3] While those who put their private information in the hands of companies would like to believe this statement, the 2017 report by Verizon sheds light on the truth of it. The annual Verizon Data Breach Investigations Report revealed that in 2016 more than 42,000 security incidents occurred.[4] Among those security incidents were "1,900 confirmed [data] breaches spanning 84 countries and 20 industries."[5] Additionally, over a billion credential sets were stolen, which is "more than three times" the rate reported in 2013.[6] "Security experts like to say that there are now only two types of companies left in the United States: those that have been hacked and those that don't know they've been hacked."[7] This statement was made in 2013 when the annual Verizon report counted 621 confirmed data breaches for the previous year.[8] With the number of confirmed data breaches nearly tripling in the three years in between reports, it is safe to say that the statement made in 2013 rings even truer today.

With data breaches come lawsuits. Because data breaches can reach hundreds, thousands, or even millions of consumers, class action lawsuits are a popular[9] and logical strategy in obtaining restitution. Accordingly, since data breaches can affect such a large number of diverse people, the cases are often filed in federal courts. The federal court system has limited jurisdiction, therefore a threshold matter in class action cases is whether plaintiffs have met Article III standing requirements.[10] While plaintiffs usually have few problems

---

3. Ross Chainey, *Davos 2015: Top Quotes From Day Two*, WORLD ECON. F. (Jan. 22, 2015), https://www.weforum.org/agenda/2015/01/davos-2015-top-quotes-from-day-two/ [https://perma.cc/4ATK-AUMC].

4. Rick Simon, *'Aha' Moments From the 'Verizon 2017 Data Breach Investigations Report'*, MCAFEE (Apr. 27, 2017), https://securingtomorrow.mcafee.com/business/data-security/aha-moments-verizon-2017-data-breach-investigations-report/ [https://perma.cc/VUP9-6TAW].

5. *Id.*

6. *Id.* "[C]redential set is the information set that is used to prove the identity of mobile users in security domains . . . ." SPRINGER, CURRENT TRENDS IN HIGH PERFORMANCE COMPUTING AND ITS APPLICATIONS 459 (Wu Zeng et al. eds., 2005).

7. Nicole Perlroth, *The Year in Hacking, By the Numbers*, N.Y. TIMES (Apr. 22, 2013, 9:10 PM), https://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/ [https://perma.cc/ZS7Z-U3EA].

8. *Id.*

9. *See* Hooker & Pill, *supra* note 2, at 34.

10. Sabrina Strong, *The Battle Over "Standing" in Class Actions*, AM. BAR ASSOC. (2014), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2014/2014_sac/2014_sac/battle_%20over_standing_in_class_action.pdf [https://perma.cc/R2WM-Y75A]. *Introduction to the Federal Court System*, U.S. DEP'T JUST.: OFFS. U.S. ATT'YS, https://www.justice.gov/usao/justice-101/federal-courts [https://perma.cc/N5QR-C5PX].

stating "a claim upon which relief can be granted,"[11] a big hurdle they face is proving that an injury has occurred.[12]

In the current digital age, technology is rapidly evolving. Unfortunately, the law does not evolve as quickly. Legislatures are slow to act and "want a consensus to develop in the public or industry before writing protective measures into law."[13] Because of this, courts bear the burden of first impression and can struggle along the way. Currently, there is a large circuit split on what constitutes an injury sufficient to satisfy Article III standing requirements.[14] The Supreme Court has yet to weigh in on this issue, resulting in conflicting precedents being set by the lower courts.[15] This Note will analyze the circuit courts' interpretations of Article III standing as it pertains to the injury requirement in data breach cases, and it will propose a universal standard which will meet such requirement. Part II of this Note provides the relevant background and development of Article III standing. Part III analyzes the current circuit split regarding the injury element of Article III standing. Part IV compares the Supreme Courts' precedent on the "injury in fact" standard to the circuit split's analysis on this requirement. Part V recommends an implementation of a statutory balancing test to fix the circuit courts' inconsistent interpretations. Part VI briefly discusses policy rationales for adopting said recommendation.

II. THE COMMON LAW DEVELOPMENT OF ARTICLE III STANDING

Because the Constitution was envisioned to be living document, the Framers sought not to spell out every aspect of the law.[16] The Constitution provides limited authority to each branch of the federal government.[17] Article III empowers federal courts with "[t]he judicial [p]ower of the United States,"[18] and while this is not defined, the Constitution specifies that this power extends only to "[c]ases" and "[c]ontroversies."[19] The courts take separation of powers seriously, trying their best not to intrude on the other branches' authority.[20]

---

11. FED. R. CIV. P. 12(b)(6).

12. *Id.* at 36.

13. Megan Dowty, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 687 (2017).

14. Fero v. Excellus Health Plain, Inc., 304 F. Supp. 3d 333, 338 (W.D.N.Y. 2018).

15. *Id.* at 338-39.

16. *See* David A. Strauss, *The Living Constitution*, U. CHI. L. SCH. (Sept. 27, 2010), https://www.law.uchicago.edu/news/living-constitution [https://perma.cc/9JDS-JZ4L].

17. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546 (2016).

18. U.S. CONST. art. III, § 1.

19. U.S. CONST. art. III, § 2.

20. *See* Raines v. Byrd, 521 U.S. 811, 819-20 (1997). "We have always insisted on

One such way to do this is to require that plaintiffs establish in their complaint that they have standing to bring a claim.[21] The Supreme Court has created an "irreducible constitutional minimum of standing," consisting of three elements: 1) the plaintiffs must have suffered an "injury in fact"; 2) that is fairly traceable to the challenged conduct of the defendant; and 3) that is likely to be redressed by a favorable judicial decision.[22] Plaintiffs have the burden of establishing these elements because they are the ones bringing the lawsuit.[23] Because standing is a threshold matter to be determined at the pleading stage, general factual allegations of each element may suffice.[24]

Put simply, standing elements require that the plaintiffs prove an injury, that the defendant caused the injury, and that the injury can be remedied by the courts. In more detail, the second element requires "a causal connection between the injury and the conduct complained of."[25] This means that that "the injury has to be fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court."[26] The third element requires that it be "likely," rather than "speculative," that the injury will be "redressed by a favorable decision."[27] This means that if the plaintiffs win, they would receive a remedy from the court that the court is capable of granting.[28] The second and third standing elements are not part of the circuit split, and therefore, they will not be discussed further in this Note.

---

strict compliance with this jurisdictional standing requirement." *Id.* at 819.

> In the light of this overriding and time-honored concern about keeping the Judiciary's power within its proper constitutional sphere, we must put aside the natural urge to proceed directly to the merits of this important dispute and to "settle" it for the sake of convenience and efficiency. Instead, we must carefully inquire as to whether appellees have met their burden of establishing that their claimed injury is personal, particularized, concrete, and otherwise judicially cognizable.

Id. at 820 (citation omitted).

21. *Id.* at 818.

22. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (internal citations omitted) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)).

23. *Id.*

24. *Lujan*, 504 U.S. at 561.

25. *Id.* at 560.

26. *Id.* (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 41-42 (1976)) (internal quotation marks omitted).

27. *Id.* at 561 (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 38, 43 (1976)) (internal quotation marks omitted).

28. DAVID SHULTZ, THE ENCYCLOPEDIA OF THE SUPREME COURT 427 (2005).

A. The Troublesome "Injury in Fact" Element

Of the three standing elements, the "injury in fact" element has proven to give the courts the most trouble, hence the circuit split. To establish an "injury in fact," plaintiffs must show that they have suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[29] All of these elements must be satisfied; it is not enough to simply plead that a statute has been violated.[30] To satisfy the "concreteness" element, the injury must be "de facto," meaning it must actually exist.[31] A concrete injury, however, does not necessarily need to be a tangible injury;[32] intangible injuries—such as freedom of speech—can be considered concrete injuries.[33] In determining intangible injuries, courts are guided by "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[34] The concrete injury must also be particularized.[35] A particularized injury means that "the injury must affect the plaintiff in a personal and individual way."[36] The courts seem to agree on how to interpret these first two elements, as evidenced by such little discussion on them.

For data breach cases, the trouble comes into play with the "actual or imminent" requirement of the "injury in fact" element. At the pleading stage, actual injuries are less likely to be disputed because plaintiffs with actual injuries can provide facts that their injuries have occurred.[37] Imminent injuries are more complex because they allow room for judicial interpretation. The Supreme Court has given vague explanations of imminence by generally stating that imminence needs to be an injury that is certainly impending and not too speculative.[38] While there is not a precise timeline for what certainly impending requires, the Supreme Court has held that plaintiffs can-

---

29. *Lujan*, 504 U.S. at 560 (internal quotation marks omitted); *see also* City of Los Angeles v. Lyons, 461 U.S. 95, 101-02 (1983); Sierra Club v. Morton, 405 U.S. 727, 734-35 (1972).

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

31. *Id.* at 1548; *see also De Facto*, BLACK'S LAW DICTIONARY (9th ed. 2009).

32. *Id.* at 1549.

33. *Id.*; *see* Pleasant Grove City v. Summum, 555 U.S. 460 (2009).

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

35. *Id.* at 1548 (holding that "[p]articularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.' ").

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

37. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (stating that tangible injuries are easier for the court to recognize).

38. *Id.* at 565 n.2.

not satisfy Article III standing requirements by merely pleading a possible future injury that might be likely to occur at some indefinite time.[39] Similarly, the Supreme Court recently held that an "objectively reasonable likelihood" that an injury will occur waters down and is inconsistent with the standing requirement that an injury be certainly impending.[40] Additionally, the Supreme Court has set precedent that fear of a future harm alone is not an adequate substitute to satisfy the "injury in fact" requirement of Article III standing.[41] The Supreme Court has also established that plaintiffs "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[42] Lastly, the Supreme Court has stated it is "reluctan[t] to endorse standing theories that rest on speculation about the decisions of independent actors."[43] On balance, these holdings represent the Supreme Court's strong stance on enforcing the irreducible constitutional minimum of standing.

As previously stated, the Supreme Court has set a precedent of strict compliance with standing requirements so as to not intrude on the other branches of the government.[44] Although this precedent should be known and followed by the lower courts, some confusion has resulted between the circuits, thus creating mixed decisions and, in some jurisdictions, a lowering of the standing requirement. Specifically, the circuits are in conflict as to what suffices as an "injury in fact" in data breach cases.

III. THE CIRCUIT SPLIT

The current circuit split is based on the interpretation of the "imminent" element for Article III standing. The differing interpretations that will be addressed in this Note are derived from recent cases from the First, Third, Fourth, Sixth, Seventh, Eighth, Ninth, and D.C. Circuits. The Sixth, Seventh, Ninth, and D.C. Circuits heed a looser standard, holding that an increased risk of identity theft is a sufficient injury to meet the standing requirement. The First, Third, Fourth, and Eighth Circuits are a little stricter, holding that an increased risk of identity theft does not comply with the standing requirements provided by the Supreme Court. This split has subsequently widened over the past ten years because more cases have been decided inconsistently due to the Supreme Court's lack of ac-

39. *Id.*

40. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410, 416 (2013).

41. *See id.* at 417; *see also* Laird v. Tatum, 408 U.S. 1, 13-14 (1972).

42. *Clapper*, 568 U.S. at 402.

43. *Id.* at 414.

44. *See* Raines v. Byrd, 521 U.S. 811, 819 (1997).

tion.[45] Due to this split and the Supreme Court's lack of guidance on this issue, lower courts are struggling to pick a side.[46]

A. Standing Based on Increased Risk of Identity Theft

The Sixth, Seventh, Ninth, and D.C. Circuits have created precedent which allows plaintiffs to pass Article III standing by pleading that they have an increased risk of identity theft (the "increased-risk-of-identity-theft standard"). Starting as early as 2007, the Seventh Circuit reversed the District Court's ruling in *Pisciotta v. Old National Bancorp*, holding that the plaintiffs—whose personal information, though not misused, had been accessed by an unauthorized third party—suffered an "injury in fact" based on the increased risk of identity theft.[47] In *Pisciotta*, hackers gained access to a marketing company's database which stored its customers' names, addresses, social security numbers, and drivers licenses.[48] The court considered the expenses that the class action plaintiffs incurred in trying to prevent their personal information from being used, and it found that the hackers were "sophisticated, intentional[,] and malicious."[49] The court held that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[50]

The increased-risk-of-identity-theft standard became a consistent precedent in the Seventh Circuit with two notable cases: *Lewert v. P.F. Chang's* and *Remijas v. Neiman Marcus*. In *Lewert v. P.F. Chang's*, hackers breached a restaurant's credit card machines in order to obtain customers' card information.[51] The plaintiffs provided that one class member in the suit had four fraudulent charges on his credit card shortly after dining at the restaurant.[52] While the class member's bank stopped the fraudulent charges before they went through, the court still held that the plaintiffs collectively suffered an injury of increased risk of identity theft because their data had been stolen and subsequently misused.[53] Considering that fraudulent

45. *See* Carefirst, Inc. v. Attias, 138 S. Ct. 981 (2018) (denying certiorari).

46. *See* Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 749-53 (W.D.N.Y. 2018).

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

48. *Id.* at 631.

49. *Id.* at 632.

50. *Id.* at 634.

51. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965 (7th Cir. 2016).

52. *Id.*

53. *Id.* at 967-68.

charges had already occurred, the court found it plausible to infer "a substantial risk of harm from the data breach" with regards to other class members because it is common for hackers to eventually make fraudulent charges or assume those customers' identities.[54] While the only information stolen was the one customer's card information, the court rationalized that this information could be used to open new cards in the customer's name and therefore cause identity theft.[55]

Similarly, in *Remijas v. Neiman Marcus*, hackers breached the store's credit card machines and obtained customers' card information, but the hackers did not obtain other information, such as social security numbers or birth dates.[56] In this case, however, 9,200 of the 350,000 cards accessed were used fraudulently.[57] But those pleading in the class action admitted that they were reimbursed for the fraudulent charges by their banks.[58] The court relied on the fact that fraudulent activity had already occurred and ruled that the plaintiffs sufficiently pled an "injury in fact" due to an increased risk of identity theft.[59]

The Sixth Circuit followed suit in *Galaria v. Nationwide*, where hackers gained access to their customers' names, social security numbers, dates of birth, and driver licenses.[60] While the class action plaintiffs did not report any fraudulent activity, the court relied on the assumption that the hackers intended to misuse the information accessed. The defendants arguably agreed, seeing as they offered their customers free credit-monitoring services and identity-theft protection for a full year.[61] Based on this rationale, the court held that it would be unreasonable to expect the plaintiffs to wait for actual misuse and that a substantial risk of identity theft was enough to satisfy the standing requirement.[62]

Additionally, the Ninth Circuit found the increased-risk-of-identity-theft standard persuasive, holding that many plaintiffs meet their burden under this standard.[63] In *Krottner v. Starbucks Corp.*, a laptop, which contained unencrypted files of approximately 97,000 employees' names, addresses, and social security numbers, was sto-

54. *Id.* at 967.

55. *Id.* The court stated no basis for why it believed credit card information would be enough to open new accounts. *Id.*

56. Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 689-90 (7th Cir. 2015).

57. *Id.* at 690.

58. *Id.* at 692.

59. *Id.* at 692-93.

60. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 385-86 (6th Cir. 2016).

61. *Id.* at 388.

62. *Id.*

63. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010).

len.[64] The plaintiffs pled that one of their class members had a fraudulent bank account opened in his name using his social security number.[65] The bank notified this class member and closed the account.[66] The court found the fraudulent account persuasive and held that an increased risk of identity theft satisfied the standing requirement.[67]

Lastly, the D.C. Circuit also adopted the increased-risk-of-identity-theft standard. In *Attias v. Carefirst*, hackers breached the company's database and obtained access to their insurance members' names, birth dates, social security numbers, and credit card information.[68] The breach, however, happened a year before detection, and the plaintiffs did not plead that any of their members had suffered fraud.[69] Regardless, the court still held that the "[p]laintiffs . . . cleared the low bar to establish their standing at the pleading stage."[70] The court rationalized that the plaintiffs suffered an increased risk of identity theft because "[w]hy else would hackers break into a . . . database and steal consumers' private information" if not to misuse that information?[71]

B. Increased Risk of Identity Theft is Insufficient to Meet the Standing Requirements

The Third, Fourth, and Eighth Circuits have created precedent which inhibits plaintiffs from passing the Article III standing threshold by simply pleading that they have an increased risk of identity theft. Collectively, these circuits have required plaintiffs to prove that the risk of identity theft is either imminent or certainly impending, which are higher thresholds than the increased-risk-of-identity-theft standard. Starting as early as 2011, the Third Circuit held that "[a]llegations of 'possible future injury' are not sufficient to satisfy Article III," but instead, "[a] threatened injury must be 'certainly impeding.' "[72] In *Reilly v. Ceridian Corp.*, hackers gained access to Ceridian's commercial businesses' payroll accounts which held personal information of those businesses' employees.[73] The personal in-

64. *Id.* at 1140.
65. *Id.* at 1141.
66. *Id.*
67. *Id.* at 1143.
68. Attias v. Carefirst, Inc., 865 F.3d 620, 622-23 (D.C. Cir. 2017).
69. *Id.* at 623.
70. *Id.* at 622.
71. *Id.* at 628-29.
72. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).
73. *Id.* at 40.

formation accessed included employee names, social security numbers, dates of birth, addresses, and bank accounts.[74] While over 27,000 employees' information was at risk due to the breach,[75] the plaintiffs did not plead that any of those employees had suffered from misuse of their information.[76] The court found this evidence extremely persuasive in deciding that the plaintiffs were not imminently at risk for identity theft, particularly because the breach happened on or about December 22, 2009, and the plaintiffs filed suit, albeit with no evidence of misuse of their information, on October 7, 2010.[77] Additionally, the court found the plaintiffs' argument of increased risk of identity theft speculative because it relied on the future actions of the hacker—an unknown third party.[78] While this case was decided before *Clapper v. Amnesty Int'l USA*,[79] it conforms with the Supreme Court's ideology of not endorsing standing theories solely based on the speculation of future decisions of independent actors.[80]

Relatedly, the Fourth Circuit was not persuaded that an increased risk of future identity theft conformed with Article III standing requirements.[81] Similar to the facts in *Krottner*, in *Beck v. McDonald*, a laptop containing personal information of 7,400 patients was likely stolen from a healthcare facility.[82] The personal information included patient names, dates of birth, the last four digits of their social security numbers, and their physical description (age, race, gender, height, and weight).[83] The court unanimously held that the plaintiffs lacked standing because they provided no evidence that the data on the laptop was ever accessed or misused.[84] The court declined to infer the intent of the laptop thief and stated that for an injury to occur, an "attenuated chain" of hypothetical events would have to happen in

74. *Id.*

75. *Id.*

76. *Id.* at 43.

77. *Id.* at 40, 46.

78. *Id.* at 42 ("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.").

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

80. *Id.*

81. Beck v. McDonald, 848 F.3d 262, 266-67 (4th Cir. 2017) (holding that an increased risk of identity theft, along with the cost of measures to protect against it, does not satisfy Article III standing).

82. *Id.* at 267. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (here, a laptop containing personal information of Starbucks employees was stolen).

83. *Beck*, 848 F.3d at 267.

84. *Id.* at 274. No dissenting opinions were voiced.

which: (1) the thief stole the laptop with the intent of accessing the plaintiffs' personal information; (2) the thief selected, from the thousands of others in the computer, the personal information of the named plaintiffs; and (3) the thief attempted to successfully use that information to steal their identities.[85] The court additionally considered that because the breach occurred in February of 2013, and this case continued into February of 2017, an imminent threat of future injury was unlikely because " 'as the breaches fade further into the past,' the [p]laintiffs' threatened injuries become more and more speculative."[86] Furthermore, the court refused to infer an increased risk of future identity theft on the basis that the healthcare facility provided free credit-monitoring services to the plaintiffs.[87] The court stated that to presume the healthcare facility believed that the plaintiffs were at risk of identity theft—since they provided these services—"would surely discourage organizations from offering these services to data-breach victims."[88]

Lastly, the Eighth Circuit created a somewhat stricter standing precedent than those set by the Third and Fourth Circuits. In *SuperValu, Inc.*, hackers accessed 1,045 of the defendants' grocery stores' computer networks that held card payment information.[89] The hackers were able to access customer names, credit or debit card account numbers, card verification value (CVV) codes, expiration dates, and personal identification numbers (PINs).[90] Out of the sixteen plaintiffs in the class action, only one of them had fraudulent charges on their account as a result of the breach.[91] In determining that most of the plaintiffs did not reach their burden of standing, the court relied on a report that the plaintiffs introduced, which stated that compromised credit or debit card information alone generally cannot be used to open new accounts.[92] Keeping this report in mind, the court dismissed all claims, except for the one plaintiff who had a fraudulent charge on his account.[93] Further, the court stated that the remaining

85. *Id.* at 275. The Fourth Circuit followed the precedent set by *Clapper* in rejecting the "attenuated chain" of events that would have to happen for the plaintiffs' information to be misused. "[A] highly attenuated chain of possibilities . . . does not satisfy the requirement that threatened injury must be certainly impending." *Clapper*, 568 U.S. at 410.

86. *Id.* at 275 (quoting Chambliss v. Carefirst, Inc., 189 F. Supp. 3d 564, 570 (D. Md. 2016)).

87. *Id.* at 276.

88. *Id.* The court feared that the organization's extension of goodwill would render them subject to suit if the plaintiffs' rationale was found to be persuasive. *See id.*

89. *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).

90. *Id.*

91. *Id.* at 767.

92. *Id.* at 770.

93. *Id.* at 774.

plaintiff could only prevail on the standing requirement for "injury in fact" if he could show that he was not reimbursed for the fraudulent charge.[94] While this court did not explicitly rule that an increased risk of identity theft was not a sufficient standard for "injury in fact," the court's holding was more consistent with the circuits who did not find an increased risk of identity theft as a sufficient standard.[95]

C. The Negative Impact of the Circuit Split

Circuit splits are hardly a favorable approach to judicial precedent because they create confusion in the lower courts. This circuit split, in particular, has created confusion in the district courts and among the circuit courts. For example, in *Fero v. Excellus Health Plan*, the District Court of New York had trouble deciding which side of the circuit split to take because their circuit court of precedent, the Second Circuit, had not yet weighed in on the issue. The court inferred that the Second Circuit would find favor with the circuits that heed the increased-risk-of-identity-theft standard because the Second Circuit favorably cited *Galaria*.[96] Further evidence that the district courts are struggling with the standing precedents is that a majority of the cases previously mentioned reversed their district court's rulings.[97] Additionally, while the Seventh Circuit already set the prece-

---

94. *Id.* at 773.

95. *See id.* at 770. The court acknowledged that other circuits have held that substantial risk of future identity theft is sufficient to constitute a threatened "injury in fact," but it nevertheless held that the plaintiffs in this case have not passed that threshold. However, if the court was truly ruling on the precedent that an increased risk of identity theft is sufficient for standing, they would have ruled that these plaintiffs had standing. The circuits upholding this standard have found standing even when a plaintiff has not had their information misused but where they think the thieves have intent to use it. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 388 (6th Cir. 2016); Attias v. Carefirst, Inc., 865 F.3d 620, 622, 628 (D.C. Cir. 2017) (where no misuse occurred, but the court questioned why hackers would otherwise try to access this information). Here, the hackers used the stolen information at least once, therefore confirming their intent and allowing the plaintiffs to reach the standing threshold based on the increased-risk-of-identity-theft standard. *In re* SuperValu, Inc., 870 F.3d 763, 767 (8th Cir. 2017).

96. *See* Fero v. Excellus Health Plain, Inc., 304 F. Supp. 3d 333, 339 (W.D.N.Y. 2018).

> [T]he Second Circuit favorably cited the Sixth Circuit's decision in *Galaria* . . . and summarized its holding as follows: "[P]laintiffs had standing to bring data breach claims when the breached database contained personal information such as 'names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers.' "

Id. (quoting Whalen v. Michaels Stores, Inc., 689 F. App'x. 89, 91 (2d Cir. 2017)).

97. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 630 (D.C. Cir. 2017); *In re* SuperValu, Inc., 870 F.3d 763, 774 (8th Cir. 2017) (reversed the district court's dismissal of one plaintiff but affirmed the dismissal as to all other plaintiffs); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 385-86 (6th Cir. 2016); Lewert v. P.F. Chang's China Bistro, Inc. 819 F.3d 963, 970 (7th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).

dent that an increased risk of identity theft is a sufficient standard, a district court in their jurisdiction still had trouble applying this standard to the case at hand. In 2007, the Seventh Circuit held in *Pisciotta* that even without the plaintiffs alleging an experience of fraud, the "injury in fact" requirement could still be satisfied if the plaintiffs could show that they would not be at an increased risk of future harm absent the defendant's actions.[98] This seems to be a low threshold, but in 2014, the district court in *Lewert* held that the plaintiffs did not reach the increased-risk-of-identity-theft standard or the certainly impending injury requirement for standing.[99] Even though some plaintiffs had incurred identity theft, no fraudulent charges were incurred.[100] This court cited to *Clapper* stating that "[s]peculation of future harm does not constitute actual injury."[101] While the Seventh Circuit reversed the district court's holding as it was inconsistent with their low threshold, this confusion shows that the lower courts are unsure about how to use the increased-risk-of-identity-theft standard, even when their jurisdiction has created binding precedent.

Likewise, the circuit split has also proved to confuse the circuit courts themselves. In *SuperValu, Inc.*, the Eighth Circuit referenced the circuit split but then stated that while courts come to different conclusions on the question of standing, it did not "need [to] . . . reconcile this out-of-circuit precedent because the cases ultimately turned on the substance of the allegations before each court."[102] This understanding of the circuit split implies that courts are working under one standard for standing, which is untrue considering the entire split is based on which standard is acceptable. Also, the circuit courts proved to be confused about the standing precedent set in *Clapper*. In *Lewert*, the Seventh Circuit stated that "[t]he plaintiffs 'should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such injury will occur.' "[103] Nowhere in *Clapper* does the Supreme Court make this assertion. If anything, the Supreme Court states that an objectively reasonable likelihood standard is insufficient to find standing.[104]

---

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

99. Lewert v. P.F. Chang's China Bistro, Inc., No. 14-cv-4787, 2014 WL 7005097, at *3 (N.D. Ill. Dec. 10, 2014).

100. *Id.*

101. *Id.* (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).

102. *In re SuperValu, Inc.*, 870 F.3d at 769.

103. *Lewert*, 819 F.3d at 966 (incorrectly quoting *Clapper*, 568 U.S. at 410).

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

Lastly, circuit splits also promote plaintiffs to forum shop.[105] Plaintiffs might be inclined to file their complaints in certain forums that have established a lower standing threshold, because these forums would likely allow their case to continue, where other forums might dismiss it at the pleading stage for lack of standing.

IV. THE SUPREME COURT'S PRECEDENT ON "INJURY IN FACT" REQUIREMENTS

As outlined in the cases discussed above, since the Supreme Court denied certiorari to many arguably injured plaintiffs on this issue, it is unclear which side of the circuit split they would follow.[106] But if past Supreme Court cases relating to Article III standing are any indication of the justices' preferences, it would likely be true that the Court would rule in favor of the lower courts that do not find the increased-risk-of-[future]-identity-theft standard sufficient. The two most recent and relevant cases that support this assertion are *Spokeo, Inc. v. Robins* and *Clapper v. Amnesty International USA*.

In *Spokeo*, the Supreme Court reversed the Ninth Circuit's determination that a plaintiff had standing because his statutory rights were being violated, and that his claim was personal and individual.[107] The Supreme Court held that simply filing suit based on a statutory right does not mean a plaintiff automatically satisfies the "injury in fact" requirement.[108] While Congress may grant the authority to sue for certain harms,[109] the plaintiff still needs to meet the "injury in fact" element to satisfy standing because the violation of a statutory right alone may result in no harm.[110] The holding in *Spokeo* could have provided the lower courts with the understanding that the Supreme Court intends to strongly enforce all elements of the Article III standing requirements.

Likewise, the Supreme Court in *Clapper* provided some guidance that the Article III standing requirements pertaining to "injury in

---

105. Forum-shopping is defined as:

> The practice of choosing the most favorable jurisdiction or court in which a claim might be heard. A plaintiff might engage in forum-shopping, for example, by filing suit in a jurisdiction with a reputation for high jury awards or by filing several similar suits and keeping the one with the preferred judge.

Forum-shopping, BLACK'S LAW DICTIONARY (10th ed. 2014).

106. *See, e.g.*, Carefirst v. Attias, 138 S. Ct. 981 (2018).

107. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544-45 (2016).

108. *Id.* at 1545.

109. *Id.* at 1549.

110. *Id.* at 1549-50.

fact" are not to be watered down by the lower courts.[111] In *Clapper*, the plaintiffs wanted a declaration claiming United States surveillance actions were unconstitutional.[112] The plaintiffs consisted of attorneys and human rights organizations who argued that their sensitive communications with individuals outside of the United States would be compromised by this surveillance.[113] While no evidence evidenced that the United States had intercepted these particular plaintiffs' communications, the plaintiffs stated that the intrusion was likely to happen in the future.[114] The plaintiffs also claimed that they had standing based on the expenditures they had incurred in trying to protect the confidentiality of their communications.[115] The Second Circuit held that the plaintiffs had standing because there was an "objectively reasonable likelihood that their communications . . . [would] be intercepted . . . at some point in the future,"[116] and because the plaintiffs are suffering present "injuries in fact" stemming from the fear of future harm.[117] The Supreme Court reversed the Second Circuit's holding and reaffirmed their strong stance that the threat of future injury must be certainly impending.[118] The Supreme Court thought the plaintiffs' fears were speculative, and not certainly impending, because they failed to offer any evidence that their communications had been monitored by the United States.[119] Additionally, the Supreme Court thought that an attenuated chain of events would have to happen for the plaintiffs' information to be misused. The Court stated: "[H]ighly attenuated chain[s] of possibilities[] do[] not satisfy the requirement that threatened injur[ies] must be certainly impending."[120] Lastly, the Court stated that the plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm."[121]

---

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

112. *Id.* at 406.

113. *Id.*

114. *Id.* at 407.

115. *Id.* at 407 (The plaintiffs claimed that to keep their communications confidential, they would have to "travel abroad in order to have in-person" communications with their clients).

116. *Id.* at 410.

117. *Id.* at 407. The "present injuries" were economic harms from paying for flights and professional harms from their diminished ability to obtain and communicate confidential information. *Id.* at 406-07.

118. *Id.* at 416.

119. *Id.* at 411.

120. *Id.* at 410.

121. *Id.* at 416.

A. Analysis of the Cases and the Stance the Supreme Courts Would Likely Take on the Circuit Split

1. Analysis of the Sixth, Seventh, Ninth, and D.C. Circuits

With the preceding discussion in mind, the Supreme Court would likely find more fault than favor with most of these circuits' analyses. Starting with the Sixth, Seventh, Ninth, and D.C. Circuits—which hold that the increased-risk-of-identity-theft standard is sufficient to meet the standing requirement—the Supreme Court would likely find favor in the balancing test used by some of these circuits. In *Lewert*, the Seventh Circuit held that the plaintiffs established an increased risk of identity theft because, after hackers accessed the restaurant's credit card database, one of the class members experienced credit card fraud.[122] The Supreme Court might find this set of events persuasive because an actual injury occurred, rather than a mere fear of a future injury which is uncertain to happen.[123] The Supreme Court suggests that while fear of a future threat alone is insufficient to create standing, claims of a specific, present, objective harm might suffice.[124] In *Lewert*, the database was breached and a class member suffered from credit card fraud; therefore, a harm was present. This harm solidified the fear of future threat because that fear was based on a concrete harm.[125] The Supreme Court, however, might be weary of finding that a class as a whole has standing where only one plaintiff has incurred an injury. Regardless, the balancing of events displayed by the Seventh Circuit would be a more favorable approach than others used on this side of the circuit split.

Not all cases, however, are as rationally reasoned. A common rationale in these circuits is the assumption that the hackers' purpose in infiltrating the databases is to steal the plaintiffs' information to misuse it.[126] Some of these cases have only the bare fact that a database was breached, yet some courts still hold that the plaintiffs are at an increased risk of identity theft. This is true even where no plaintiff had claimed fraud as a result of the breach.[127] These circuits rely

122. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

123. *See Clapper*, 568 U.S. at 417-18 (referencing Laird v. Tatum, 408 U.S. 1, 11 (1972)).

124. *Id.* at 418.

125. *Lewert*, 819 F.3d at 967.

126. *See, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 628-29 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 388 (6th Cir. 2016); *Lewert*, 819 F.3d at 967; Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).

127. *See, e.g.*, *Attias*, 865 F.3d at 626; *Galaria*, 663 F. App'x. at 388; *Pisciotta*, 499 F.3d at 634.

on this assumption to make the argument that the plaintiffs are at an increased risk of identity theft because "[w]hy else would hackers break into a . . . database and steal consumers' private information" if not to steal the plaintiffs' information and commit identity theft.[128] While common sense might find this reasoning persuasive, hackers have proven to have different motives when infiltrating databases. For instance, in 2015, a group called "Impact Team" hacked the Ashley Madison website.[129] Ashley Madison was an online dating website which glorified having affairs, and accordingly, the website connected users interested in extramarital affairs.[130] While the website charged for user access and therefore contained payment information in its database, the hackers let it be known immediately that their intent in hacking the system was solely to shut it down for moral reasons.[131] The hackers gave the website owners a timeframe to shut down operations, and when the threat was ignored, the hackers released information for over thirty-two million users.[132] This information contained usernames, first and last names, email addresses, passwords, credit card information, addresses, phone numbers, and transaction records.[133] The hackers were sophisticated and had the information necessary to defraud the users, but they had moral rather than monetary reasons for releasing the information. These types of hackers are known as hacktivists, and they have been involved in morally-motivated hacks as early as the 1990s.[134]

Additionally, the Supreme Court might find fault in the D.C. Circuit's holding in *Attias*. In *Attias*, hackers obtained personal information such as birth dates, social security numbers, and credit card information.[135] While no class members provided evidence of fraud, the court held that the plaintiffs "cleared the low bar to establish

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

129. Eric Basu, *Cybersecurity Lessons Learned from the Ashley Madison Hack*, FORBES (Oct. 26, 2015, 11:55 AM), https://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#19b883264c82 [https://perma.cc/6K27-BGVT].

130. *Id.*

131. *Id.* ("The hacking group purposely targeted the site because they profit 'off the pain of others,' the stated reason for the group's attack on the site.").

132. *Id.*

133. Swati Khandelwal, *Ashley Madison to Pay $11.2 Million to Data Breach Victims*, HACKER NEWS (July 16, 2017), https://thehackernews.com/2017/07/ashley-madison-data-breach.html [https://perma.cc/58T2-W4XW].

134. Elizabeth Falconer, *Ashely Madison Breach: Hacktivists or Criminals?*, N.C. J.L. & TECH. (Sept. 17, 2015), http://ncjolt.org/ashley-madison-breach-hacktivists-or-criminals/ [https://perma.cc/Y38D-2VKB]. In the 1990s, a hacking group called "Cult of Dead Cow" breached databases to "leverage[] technology to advance human rights and protect the free flow of information." *Id.* (internal quotation marks omitted).

135. Attias v. Carefirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017).

their standing at the pleading stage."[136] The Supreme Court has set a precedent of strict compliance with standing requirements so as to not intrude on the other branches of government, and therefore, would likely find fault with this circuit's treatment of Article III standing.[137] While the pleading stage presents a lower hurdle than the trial stage,[138] it is one of the most important stages of litigation because it ensures that the judiciary is not overstepping its power.[139] In *Attias*, the plaintiffs only pled that a breach occurred and reasoned that the hackers must have intended to misuse the information they obtained because "[w]hy else would hackers break into a . . . database and steal consumers' private information."[140] Further, the breach had occurred nearly one year before the company noticed the intrusion.[141] The Supreme Court would likely find that if fraud did not occurr in the one year before detection of the intrusion, then future harm would not be imminent and therefore does not satisfy Article III standing.

Lastly, the Supreme Court would likely find fault in the Sixth Circuit's holding in *Galaria*. The Sixth Circuit held that the plaintiffs were at an increased risk of identity theft because hackers gained access to personal information that could be used to open new accounts.[142] This court assumed the hackers would use the information to defraud the plaintiffs and found standing on the basis that the plaintiffs incurred an "injury" due to the time and money spent monitoring their accounts for fraud.[143] The court gave little value to the

---

136. *Attias*, 865 F.3d at 622.

137. *See* Raines v. Bryd, 521 U.S. 811, 819 (1997).

138. *See* Alexander A. Reinert, *The Burdens of Pleading*, 162 U. PA. L. REV. 1767, 1772 (2014). *Ashcroft v. Iqbal* created:

> [A] two-step process for evaluating the sufficiency of a complaint. First, courts must review each allegation in a complaint and exclude from consideration those allegations stated in a 'conclusory' fashion. Second, and consistent with *Twombly*, courts must conduct a plausibility analysis that assesses the fit between the nonconclusory facts alleged and the relief claimed. The judge may assess plausibility by calling on her 'judicial experience and common sense . . . .'

Id. (footnotes omitted). "In sum . . . plausibility pleading depends on the judge to conduct a preliminary evaluation of the likelihood of a claim's success." *Id.* This is a lower standard than the burden of proof at trial, because at trial, the plaintiffs have the affirmative duty to prove the facts alleged in the complaint. *See Burden of Proof*, BLACK'S LAW DICTIONARY (10th ed. 2014).

139. *See* Raines v. Byrd, 521 U.S. 811, 819-20 (1997). "We have always insisted on strict compliance with this jurisdictional standing requirement." *Id.* at 819.

140. *Attias*, 865 F.3d at 628-29.

141. *Id.* at 623.

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

143. *Id.* at 388 ("Where [p]laintiffs already know that they have lost control of their data, it would be unreasonable to expect [p]laintiffs to wait for actual misuse—a fraudulent

fact that the defendant paid for one year of credit-monitoring services for the plaintiffs, as the court considered the plaintiffs paying to monitor their accounts an injury.[144] The Supreme Court would likely find great flaws in this case because it has set strict precedent that plaintiffs cannot manufacture standing by presenting self-inflicted injuries alone.[145] Since no fraud actually occurred, and the Sixth Circuit strictly relied on the intentions of third parties, paired with the plaintiffs' self-inflicted injuries, the Supreme Court would likely take a strong stance against this type of standing precedent because it is completely contrary to its opinion in *Clapper*.[146]

These circuits, which have held Article III standing to be satisfied by proving an increased risk of identity theft, have seemingly lowered the standing threshold. While some circuits have ruled consistently with the threshold requirements set by the Supreme Court,[147] others are allowing plaintiffs to have standing with the bare assertion that a data breach has occurred.[148] The reasoning of these circuits—that those who breach databases containing personal information must have the intent of misusing it—blatantly opposes the Supreme Court's stance that that it will not "endorse standing theories that rest on speculation about the decisions of independent actors."[149] Additionally, while some circuit courts find it unreasonable to have plaintiffs wait for fraud to occur,[150] the Supreme Court would find fault in watering down the standing threshold by not following the

charge on a credit card, for example—before taking steps to ensure their own personal and financial security . . . .").

144. *See id.* at 386.

145. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013).

146. *See id.* ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."). *See also id.* at 414 ("We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.").

147. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016). This court balanced a data breach occurrence on a credit card database with a customer's credit card subsequently incurring fraud to come to the assertion that other members of the class are at an increased risk of identity theft. *Id.* at 967. This is consistent with the Supreme Court's analysis that fear of future injury needs to be imminent. *See Clapper*, 568 U.S. at 418 (citing Laird v. Tatum, 408 U.S. 1, 13-14 (1972)). If some customers are already suffering from fraud, then it is a rational argument that others might imminently incur the same fate.

148. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017); *Galaria*, 663 F. App'x. at 388; Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

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

150. *See Lewert*, 819 F.3d at 966. This court somehow misquotes *Clapper* by stating, "[t]he plaintiffs 'should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an "objectively reasonable likelihood" that such injury will occur.' " *Id.* Nowhere in *Clapper* does the Supreme Court make this assertion. If anything, the Supreme Court states that an objectively reasonable likelihood standard is insufficient to find standing. *See Clapper*, 568 U.S. at 410.

imminent or certainly impending standard for a future injury, because in effect, these circuits are intruding on the power of other branches of government.[151]

2. Analysis of the Third, Fourth, and Eighth Circuits

Switching to the other half of the circuit split, the Third, Fourth, and Eighth Circuits have created precedent which refuses to allow plaintiffs to pass the Article III standing threshold by simply pleading that they have an increased risk of identity theft. These courts hold that plaintiffs must show imminent or certainly impending threats of future injury.[152] The Supreme Court would likely find that these circuits heed the Court's precedent set for determining standing in future injury cases. Looking at *Reilly v. Ceridian Corp.*, the Supreme Court would agree that these plaintiffs did not have standing because, while personal information (such as social security numbers, names, and dates of birth) were accessed by hackers in December of 2009, fraud was not reported when the plaintiffs filed their complaint in October of 2010.[153] Additionally, it was unknown if the hackers read, copied, or understood the data;[154] thus, the court chose to follow the Supreme Court's precedent and held it was too speculative to base standing on the future actions of unknown third parties.[155]

Likewise, the Supreme Court would likely agree that the Fourth Circuit was following the proper standing precedent. In *Beck*, the Fourth Circuit refused to find standing when the plaintiffs based their entire argument on the future actions of unknown third parties.[156] Similar to *Krottner*, a laptop was stolen containing the plaintiffs' personal information, specifically their social security numbers,

151. *See Clapper*, 568 U.S. at 410, 416. "[T]he Second Circuit's 'objectively reasonable likelihood' standard [that plaintiffs will suffer an injury in the future] is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.' " *Id.* at 410. *See* Raines v. Bryd, 521 U.S. 811, 819 (1997).

152. *See In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017) (using the imminent standard for standing); Beck v. McDonald, 848 F.3d 262, 270-71 (4th Cir. 2017) (using the imminent standard for standing)*;* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (emphasis added) (using the *certainly impending* standard for standing).

153. *Reilly*, 664 F.3d at 40-42.

154. *Id.* at 40.

155. *Id.* at 42. *See also Clapper*, 568 U.S. at 402 ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."); *see also id.* at 414 ("We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors.").

156. *Beck*, 848 F.3d at 275.

dates of birth, and names.[157] *Krottner* is distinguishable, however, because the intent of the hacker could be inferred. Shortly after the laptop was stolen, the hacker attempted to open a fraudulent account in one of the plaintiff's names.[158] In *Beck*, however, no fraud was reported, which requires the court to assume the intent of the hacker.[159] This assumption would go against the precedent set forth in *Clapper*; therefore, the Supreme Court would likely agree that bare allegations of theft of an item with personal information on it is not enough to satisfy the Article III standing requirement of "injury in fact."[160]

Lastly, the Supreme Court would also likely agree that the Eighth Circuit is upholding the strict standards of Article III standing. In *SuperValu, Inc.*, hackers accessed customer card information by hacking into the store's payment database.[161] The information obtained was limited to customer names, credit or debit card account numbers, expiration dates, CVV codes, and PINs.[162] The court took into consideration that one member of the class had experienced fraud, but it nonetheless held that all other members did not have standing because the hackers did not have access to information to create new accounts.[163] Therefore, any future injury would likely be limited to credit or debit card fraud and not identity theft.[164] It can also be inferred that this court did not find the future threat imminent because the breach happened almost a year before the plaintiffs filed suit, and because only one fraudulent transaction had occurred with one class member.[165] Additionally, to remain eligible for standing, the plaintiff the court granted standing to, must prove that he was not reimbursed for the fraudulent charges.[166]

V. PROPOSED "INJURY IN FACT" STANDARD TO RECTIFY THE CIRCUIT SPILT

The Supreme Court has stated that the purpose of imminence is "to ensure that the alleged injury is not too speculative for Article III

157. *Id.* at 267. *See also* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (A laptop was stolen containing personal information of Starbucks employees).

158. *Krottner*, 628 F.3d at 1141.

159. *Beck*, 848 F.3d at 274.

160. *See Clapper*, 568 U.S. at 410 ("[H]ighly attenuated chain[s] of possibilities [do] not satisfy the requirement that threatened injury must be certainly impending.").

161. *In re* SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).

162. *Id.*

163. *Id.* at 770.

164. *Id.* at 771.

165. *Id.* at 766-67 (The initial breach occurred in August of 2014, and the plaintiffs filed their consolidated complaint in June of 2015).

166. *Id.* at 773.

purposes–that the injury is *certainly* impending."[167] Although the Supreme Court set precedent stating that relaxing this standing requirement is improper, the Sixth, Seventh, Ninth, and D.C. Circuits are having trouble following suit.[168] Because the circuits are still having trouble with the "injury in fact" requirement of Article III standing, even with Supreme Court's precedent, this Note recommends that statutory provisions be adopted for the courts to follow. These provisions will only cover the imminent standard for future injuries, which should be followed for data breach class action cases. As noted in *Spokeo*, Congress is well positioned to identify intangible harms that meet the minimum requirements of Article III.[169] The likelihood of future injuries is seemingly an intangible harm because the injuries do not actually exist yet.[170] Since these injuries are not present, they are harder to recognize but can still be considered concrete for the purposes of Article III standing.[171]

By combining the circuit courts' analysis and the precedent set by the Supreme Court, a statutory solution for federal standing requirements can be developed, and accordingly, should be implemented by means of a balancing test. This Note proposes the following balancing test:

> 1). As required by all courts, some sort of breach or unauthorized access of personal information must be established.[172]
>
> 2). A determination of whether the type of information stolen would allow the unauthorized accessor the ability to open fraudulent accounts.[173] If the information is simply credit card infor-

---

167. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 565 (1992)).

168. *See id.* at 416.

169. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

170. *See id.* at 1548-49.

171. *Id.* at 1549.

172. *See* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (holding an injury has not occurred when there is only a fear of a future data breach). This court cites to the circuit split but states that in each case plaintiffs' data had been accessed by one or more unauthorized third parties. *Id.*

173. *In re* SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017) ("The type of data compromised in a breach can effectively determine the potential harm that can result." (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007), http://www.gao.gov/assets/270/262899.pdf [https://perma.cc/8WS2-FVWD])). This court states that credit card information alone—particularly information involving account numbers, names, CVVs, expiration dates, and PINs—leave plaintiffs in "little to no risk that anyone will use the [c]ard [i]nformation stolen in these data breaches to open unauthorized accounts in the plaintiffs' names, which is 'the type of identity theft generally considered to have a more harmful direct effect on consumers.' " *Id.* (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *supra*).

mation, in which new accounts cannot be created, then the plaintiffs need to provide evidence that they have incurred fraud and that their card issuers have not reimbursed them.[174] Otherwise, standing should not be granted.

3). The courts cannot infer the intent of third parties who improperly access personal information.[175] The courts will need some form of substantive proof, like personal information being hacked and subsequently used in some way.[176] This requirement will prove that the intent of the third parties was to misuse the information.

4). The courts can take into consideration expenditures that the plaintiffs have incurred in trying to protect their accounts and identities, but this cannot be the sole source of injury arising from the breach.[177]

5). The courts must consider the time frame in which the breach occurred and when the complaint was filed. Certainly impending or imminent standards for standing need to be followed. While hackers can sit on information for weeks before misusing it,[178] a year or longer between the breach and the fraudulent activity is not imminent.[179]

---

174. *In re* SuperValu, Inc., 870 F.3d at 773 (holding that the plaintiff who experienced credit card fraud had standing, but if evidence proved that he had been reimbursed for the fraudulent charges, standing no longer exists); *see also* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696-97 (7th Cir. 2015). While some card companies offer its customers zero liability policies, under which the customer is not liable for fraudulent charges, zero liability is not a federal requirement. The courts should not assume that all card companies will reimburse their customers. *Id.* at 697.

175. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013). *See id.* at 402. The Supreme Court is reluctant to make speculations about the decisions of independent actors. *Id.* at 414. *See also* Falconer, *supra* note 134 (Some hackers have a moral purpose behind accessing personal information, such as the "hacktivists" in the Ashley Madison data breach).

176. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42-43 (3d Cir. 2011). This court found that a data breach where hackers had access to only the plaintiffs' personal information (such as social security numbers, dates of birth, and names) was not enough to prove an injury for Article III standing purposes. The court declined to infer the intent of the hackers and stated that a chain of events would have to occur in which the hackers read and understood the information, intended to use the information, and then successfully used the information to the plaintiffs' detriment. This chain of occurrences was too speculative to confer standing. *Id.* at 46.

177. *Clapper*, 568 U.S. at 402 ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

178. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015). A plaintiff used her card in the store in December of 2013 and found fraudulent charges on her card in January of 2014. *Id.* at 691.

179. *See* Beck v. McDonald, 848 F.3d 262, 274-75 (4th Cir. 2017) ("[T]he passage of time without a single report from [p]laintiffs that they in fact suffered the harm they fear must mean something." (quoting *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015))).

> 6). Lastly, the court needs to consider if any fraud has occurred and on how many instances.[180]

All in all, these elements are meant to reduce the number of complaints making it past the pleading stage due to certain circuits lowering the "injury in fact" requirement of Article III standing. While fraud is not required to prove a future injury, some sort of substantive proof that the hackers intended to access the information to misuse it needs to be present; otherwise, the future injury is too speculative. While these standards might stifle plaintiffs' opportunity to proceed with their cases, the standards proposed are meant to preserve the court system for those plaintiffs who truly have future injuries, as well as properly extract funds from those companies who were trusted in preserving the confidentiality of the plaintiffs' personal information. Although not every case can be heard, there needs to be a substantial limit to the ones passing through without merit.

A. Policy Considerations for the Statutory Proposed Standard

One of the biggest policy reasons for creating a uniform standard that limits the amount of cases allowed to continue past the pleading stage is the fact that the court systems are overloaded. Recently, as many as 330,000 civil cases were pending in the federal district courts.[181] According to the Administrative Office of the United States Courts, this large number of pending cases is up nearly 20 percent since 2004.[182] Further, over 30,000 cases have been waiting for their day in court for three years or more.[183] While the Seventh Amendment provides plaintiffs in civil cases with the right to a jury,[184] the Sixth Amendment give defendants in criminal cases the right to a speedy trial.[185] Due to these standards, "[c]riminal cases often displace and delay civil disputes, creating a backlog."[186] As such, district court judges are struggling with this issue. One judge stated:

> Over the years I've received several letters from people indicating, 'Even if I win this case now, my business has failed because of

180. *See In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017).

181. Joe Palazzolo, *In Federal Courts, the Civil Cases Pile Up; Record Number of Pending Actions Delays Some Suits for Years*, WALL ST. J. (Apr. 6, 2015, 2:09 PM), https://www.wsj.com/articles/in-federal-courts-civil-cases-pile-up-1428343746 [https://perma.cc/737S-SUH2].

182. *Id.*

183. *Id.*

184. U.S. CONST. amend. VII.

185. U.S. CONST. amend. VI.

186. *Id.*

> the delay. How is this justice?' . . . And the simple answer, which I cannot give them, is this: It is not justice. We know it."[187]

The courts need legislative help to implement a uniform system to weed out the cases that cannot allege an injury from the cases with merit.

Another policy consideration in favor of this balancing test is that class action cases tend to benefit too many uninjured parties.[188] As shown in this circuit split, a whole class can gain access to the court system because one plaintiff suffered an injury, while other, similar cases may be denied access to the courts .[189] However, even if the suit prevails or decides to settle, "very few potential class members ever see a dime from class actions supposedly brought on their behalf."[190] Lawyers—another group of uninjured parties—always get paid if the case is awarded an amount of money, regardless of if the case is resolved at trial or in settlement.[191] The proposed balancing test above would help eliminate some of these problems by requiring the courts to consider if the class is certifying itself based on one isolated instance of fraud.[192] This consideration will allow the actual injured party to seek out the court system individually and prevent large awards that ultimately go to a few class members and lawyers.

Additionally, this balancing test will save companies and shareholders the expense of litigating meritless cases. When companies are hit with a lawsuit, it affects the shareholders as well.[193] It has become common for businesses to try to settle these lawsuits for fear

---

187. *Id.* (quoting Judge Lawrence J. O'Neill, sitting on the Eastern District of California) (internal quotation marks omitted).

188. *See* Daniel Fisher, *Study Shows Consumer Class-Action Lawyers Earn Millions, Clients Little*, FORBES (Dec. 11, 2013, 8:46 AM), https://www.forbes.com/sites/danielfisher/2013/12/11/with-consumer-class-actions-lawyers-are-mostly-paid-to-do-nothing/#35b702651472 [https://perma.cc/LTN4-6XPX].

189. *See* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 969-70 (7th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010).

190. *See Unstable Foundation: Our Broken Class Action System and How to Fix It*, U.S. CHAMBER: INST. FOR LEGAL REFORM (Oct. 24, 2017), http://www.instituteforlegalreform.com/research/unstable-foundation-our-broken-class-action-system-and-how-to-fix-it [https://perma.cc/4W8F-LAEL].

191. *See* Daniel Fisher, *supra* note 188 ("When consumer class actions do settle, lawyers usually negotiate a deal that pays them and their named plaintiffs well, but delivers little to nothing to their other clients.").

192. *See In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017).

193. ANDREW J. PINCUS, WHAT'S WRONG WITH SECURITIES CLASS ACTION LAWSUITS?: THE COST TO INVESTORS OF TODAY'S PRIVATE SECURITIES CLASS ACTION SYSTEM FAR OUTWEIGHS ANY BENEFITS, U.S. CHAMBER: INST. FOR LEGAL REFORM (Feb. 5, 2014), http://www.instituteforlegalreform.com/uploads/sites/1/Securities_Class_Actions_Final1.pdf [https://perma.cc/43HZ-Y45N].

that juries will give draconian awards.[194] Even settling the case can result in a large sum of money being paid out, depending on how many members are involved in the class action.[195] In most of the cases mentioned in this Note, the defendant companies immediately offered a year of free credit-monitoring services to the clients whose personal information had been breached.[196] The proposed balancing test helps incentivize this behavior by allowing companies to focus their resources on preventing fraud rather than focusing on potential threats of litigation due to a lower standing threshold. Further, the balancing test gets rid of the analysis that if companies provide free credit-monitoring services, then they must believe the third party who accessed the personal information intends to misuse it.[197]

Lastly, as previously mentioned, a circuit split can lead to forum-shopping.[198] When possible, plaintiffs would likely pick the forum which would grant them standing to move forward with their case.[199] This could lead to plaintiffs filing their cases in certain forums, which undoubtedly are already swamped with cases. Having a uniform standing requirement among the circuits would help eliminate this possibility.

B. Impact the Proposed Balancing Test Will Have on the Federal Courts

Under the current system, judicial review at the pleading stage requires the determination of whether the substantive merits of the case, as presented in the complaint, meet the standing requirements set forth by common law.[200] As stated throughout this Note, judges have a hard time determining where the line is for meeting the standing requirements. The balancing test essentially gets rid of the watered-down standard—that an increased risk of identity theft is sufficient to satisfy the "injury in fact" requirement of Article III standing— promoted by the Sixth, Seventh, Ninth, and D.C. Cir-

194. Gregory Brown, *What are Class Actions and How Do They Impact Businesses?*, BROWN & CHARBONNEAU, LLP (July 25, 2017), https://www.bc-llp.com/class-actions-impact-businesses [https://perma.cc/3SNR-NZVT].

195. *Id.*

196. *See* Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x. 384, 385 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).

197. *See Galaria*, 663 F. App'x. at 388; *cf. Beck*, 848 F.3d at 276 (holding that adopting this rationale would discourage companies from providing such goodwill services because it would cause them liability in court).

198. *See supra* note 105 and accompanying text.

199. *See supra* note 105 and accompanying text.

200. *See* Reinert, *supra* note 138.

cuits.[201] Thus, the balancing test would dispose of more cases at the forefront and promote efficiency. Statistics have shown that a majority of cases already do not get to trial; specifically, in 2003, the number of civil cases in federal court was down to 1.7 percent.[202] This number does not improve in state courts, where in 2010, 0.2 percent of circuit court cases in Florida made it to trial.[203] Ultimately, this balancing test would save the plaintiffs, defendants, and the courts time and money.

VI. CONCLUSION

Hackers infiltrating personal information stored in companies' databases is expected to increase in the coming years.[204] In 2015, businesses were the target of 40 percent of security breaches.[205] With these statistics expected to grow higher in coming years,[206] it is all the more necessary to implement a uniform standing policy for data-breach class action cases. In the midst of rapidly changing technological advances—which have allowed hackers easier access to consumers' personal information—a circuit split has occurred between the Sixth, Seventh, Ninth, and D.C. Circuits and the Third, Fourth, and Eighth Circuits.[207] The Sixth, Seventh, Ninth, and D.C. Circuits have adopted a relaxed standing requirement which states that plaintiffs need only to prove an increased risk of identity theft to satisfy Article III standing. While the Supreme Court has set precedent that lowering this minimum threshold for standing is improper,[208] the circuit courts have continued to rationalize a way around it. The Third, Fourth, and Eighth Circuits follow more closely the Supreme Court's precedent, but since the circuits are operating under different standing requirements, opposing precedents remain among the courts.

One way to fix this circuit split is to implement a uniform statutory standing requirement. The proposed requirement consists of a

---

201. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 628-29 (D.C. Cir. 2017); *Galaria*, 663 F. App'x. at 388-89; Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016); *Remijas*, 794 F.3d at 696; *Krottner*, 628 F.3d at 1143 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

202. *See* Reinert, *supra* note 138.

203. *See* J. Mason Williams IV, *What are the Odds a Case is Going to Trial?*, WIDERMAN MALEK (Jan. 3, 2013), https://legalteamusa.net/civillaw/2013/01/03/what-are-the-odds-a-case-is-going-to-trial/ [https://perma.cc/28NG-PGQC].

204/ *See* John DiGiacomo, *Top Data Breaches of 2018: Hackers Find New Methods*, REVISION LEGAL (Aug. 27, 2018), https://revisionlegal.com/data-breach/2018-statistics/ [https://perma.cc/63J5-NW4U].

205. *Id.*

206. *Id.*

207. *See supra* Part III.

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

balancing test in which the courts are to weigh all applicable elements in deciding whether plaintiffs have met the standing threshold. This balancing test is intended to coincide with the precedent already provided by the Supreme Court, and it attempts to set boundaries that the Supreme Court would likely follow had they granted certiorari to review the cases involved in the circuit split. With the confusion displayed by the district and circuit courts, the legislature would be the most appropriate governing body to set a uniform standing standard in motion.