Michigan Law Review

Volume 114 | Issue 8

2016

A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After *Clapper v. Amnesty International USA*

Thomas Martecchini
University of Michigan Law School

NOTE

A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After *Clapper v. Amnesty International USA*

*Thomas Martecchini**

Following a data breach, consumers suffer an increased risk of identity theft because of the exposure of their personal information. Limited protection by data-breach statutes has made it difficult for consumers to seek compensation for these injuries and penalize the companies that fail to protect their information, leading consumers to bring common law claims in court. Yet courts have disagreed about whether an increased risk of identity theft qualifies as an injury-in-fact under Article III standing principles: the Seventh and Ninth Circuits have approved of increased risk standing, while the Third Circuit has rejected it. The Supreme Court has further clouded the issue with its recent examination of the injury-in-fact requirement in Clapper v. Amnesty International USA. *This Note argues that courts should recognize increased risk standing in certain circumstances, even after* Clapper*, by applying a framework examining certain key factors in data breaches. It further contends that courts, in implementing this framework, should borrow certain elements from the damages analysis for common law claims to prevent the prompt dismissal of claims based on increased risk when considered on their merits.*

Table of Contents

Introduction 1472
I. A Split in Approaches Toward Increased Risk Standing 1475
A. *Standing Principles* 1475
B. *Increased Risk in Cases Decided Before* Clapper 1476
II. *Clapper*'s Effect in the Data-Breach Context 1478
A. Clapper*'s Place in the Article III Standing Framework* 1479
B. *District Courts' Conflicting Interpretations of* Clapper 1483
1. Courts Adopting *Clapper*'s Stricter Standard 1483
2. Courts Rejecting *Clapper*'s Effect 1484
3. Resolution of Conflicting Approaches 1486

* J.D. Candidate, May 2017, University of Michigan Law School. I would like to thank Ryan Rott and all on the *Michigan Law Review* team—particularly Danielle Kalil-McLane, Kate Canny, Sommer Engels, Chance Hill, and Andrew Robb—for helping make this Note what it is; my family and friends, especially my parents and Niko, Chris, and Nick, for their lifelong support; and Lauren, for loving me and keeping me sane throughout the writing process.

III. Problems with Identifying an Appropriate Standing Framework 1487
A. *Comparison to Medical-Monitoring and Environmental Cases* 1488
B. *Damages-Related Limitation* 1491
IV. Proposed Standing Framework 1492
A. *Factor-Based Framework* 1493
B. *Preferred Method of Implementation* 1494
Conclusion 1496

Introduction

We live in a world controlled more than ever before by the cybersphere. The amount of data stored on networks has increased exponentially in recent years,[1] changing the way people interact and conduct business.[2] Much of this data is personal information, which consumers must provide for even basic transactions.[3] As a result, "the intimate details of our lives"—addresses, birth dates, Social Security numbers, and credit card and bank account information—are now stored in online databases.[4]

Frequently exchanging personal information can lead to significant consequences.[5] As the amount of online data has increased, so have instances of computer hacking and theft of consumers' personal information.[6] Hacking incidents aside, breaches often follow simple mistakes by employees.[7] As a result, breaches now occur several times a week.[8] Indeed, a recent report by

1. Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 Tex. Wesleyan L. Rev. 183, 184 (2011).

2. Jessica R. Nicholson & Ryan Noonan, U.S. Dep't of Commerce, ESA Issue Brief No. 01-14 1, Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services (2014), http://www.esa.doc.gov/sites/default/files/digitaleconomyandtrade2014-1-27final.pdf [http://perma.cc/B26E-8S47].

3. Rancourt, *supra* note 1, at 184; Elizabeth T. Isaacs, Comment, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 Okla. L. Rev. 519, 519 (2015).

4. Carolyn A. Deverich et al., *Into the Breach*, L.A. Law., Feb. 2012, at 27, 27, http://www.lacba.org/docs/default-source/lal-back-issues/2012-issues/february-2012.pdf [https://perma.cc/M8JT-KEA9].

5. *See* Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 Am. U. L. Rev. 1365, 1367–68 (2013).

6. Rancourt, *supra* note 1, at 184.

7. *See, e.g.*, Experian, 2015 Second Annual Data Breach Industry Forecast 6 (2015), https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf [http://perma.cc/ZH93-WEUN]; Elizabeth Weise, *Corporate Data Breaches Grow 'Exponentially'; 43% of Companies Hit in Past Year, Study Says*, USA Today, Sept. 24, 2014, at 3B, http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/16106197/ [http://perma.cc/2DDH-P7LG].

8. *See Chronology of Data Breaches: Security Breaches 2005 – Present*, Privacy Rts Clearinghouse, https://www.privacyrights.org/data-breach [perma.cc/TZ9A-SBCR]. These figures likely underestimate the occurrence rate for breaches, since they do not account for

an organization that compiles information about confirmed data breaches showed that the organization tracked a record number of breaches in 2014—18 percent higher than the previous record, and an increase of more than 27 percent from 2013.[9] Data breaches have thus risen to unprecedented levels during "the [d]ecade of the [d]ata [b]reach."[10]

In light of these broad risks, companies have had to fundamentally reorient their approaches to data security. Some have done just that, increasing investments in security technology or creating data-breach response plans.[11] But two factors reduce the impact of those changes on data breaches. First, failure to frequently review and update data-breach response plans often renders them ineffective.[12] Second, new technologies present new opportunities for data breaches, and companies may not be able to properly account for these developments.[13] Moreover, many other businesses still remain in denial about the threat of data breaches, either failing to implement any data-security changes or making only nominal modifications.[14]

Customers suffer enormous harms because of data breaches, including increased risk of identity theft.[15] They have a limited ability, however, to seek redress for these injuries or to compel businesses to provide better data security. There are no unified federal data-security regulations, so state breach-notification statutes are the primary means for holding businesses accountable for their role in the breaches.[16] Yet differences between the state requirements create a "patchwork" that varies by state,[17] making results unpredictable and inconsistent. This statutory scheme thus provides limited protection for consumers in the wake of data breaches.

As a result, consumers have increasingly turned to litigation against the companies responsible for protecting their information—from retail stores to data-storage companies—to address their injuries. These cases are usually

---

unreported and undiscovered breaches. Todd H. Greene et al., *A Crash-Course in Data-Security Regulation and Litigation*, ACC DOCKET, Sept. 2015, at 92, 94.

9. *Identity Theft Resource Center Breach Report Hits Record High in 2014*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html [perma.cc/2Q5S-9PFU].

10. Ronald I. Raether, *Ten Years Later: Data Governance in the Decade of the Data Breach*, FED. LAW., Sept. 2015, at 40, 40.

11. EXPERIAN, *supra* note 7, at 2.

12. *See* Weise, *supra* note 7 ("[F]ew companies seem to take the need seriously. . . . Thirty-seven percent hadn't reviewed or updated their [data-breach response] plan since it was first put in place.").

13. EXPERIAN, *supra* note 7, at 4–5, 7 (discussing data-security problems posed by cloud services, digitalization of hospital patients' records, and the Internet of Things).

14. Raether, *supra* note 10, at 41; *see also* Weise, *supra* note 7.

15. Deverich et al., *supra* note 4, at 27–28.

16. Greene et al., *supra* note 8, at 94–95.

17. Julie A. Heitzenrater, *Data Breach Notification Legislation: Recent Developments*, 4 I/S 661, 663–66 (2009).

class actions since individual consumers incur only small monetary damages.[18] Consumers may assert common law claims like negligence or breach of contract, or claims that arise under consumer-protection statutes.[19] Those claims are based on injuries related to consumers' increased risk of identity theft, with damages including costs for credit monitoring purchased to guard against identity theft.[20]

Courts have disagreed on whether increased risk of identity theft is an injury-in-fact sufficient to create standing, and the Supreme Court has not yet addressed the issue. Departing from an initial trend in district courts to deny standing based on increased risk, the Seventh and Ninth Circuits—in *Pisciotta v. Old National Bancorp*[21] and *Krottner v. Starbucks Corp.*,[22] respectively—recognized standing based on increased risk.[23] The Third Circuit rejected that approach in *Reilly v. Ceridian Corp.*,[24] which the Supreme Court appeared to indirectly approve through its discussion of future harm in *Clapper v. Amnesty International USA*.[25] Yet *Clapper*'s applicability is unclear, given its different factual context.[26] Indeed, district courts apply *Clapper* to data-breach cases inconsistently,[27] clouding the future status of increased risk standing.

This Note argues that courts should adopt a framework to permit plaintiffs in certain data-breach cases to satisfy the injury-in-fact element of the standing analysis by alleging an increased risk of identity theft. Part I examines the purposes of the standing doctrine and the contrasting approaches to standing in *Pisciotta*, *Krottner*, *Reilly*, and similar district court cases. Part II contends that *Clapper*, when considered in light of Article III standing precedent, simply reiterated the existing standing inquiry instead of imposing stricter requirements. Part III identifies flaws in the current approach to increased risk standing in data-breach cases and contends that an appropriate framework should account for these problems. Part IV then proposes that courts—not Congress—resolve the post-*Clapper* split by adopting an analysis that focuses on the nature of the data breach and thus anticipates and avoids both of the concerns raised in Part III.

---

18. J. Thomas Richie, *Data Breach Class Actions*, GPSolo, Sept./Oct. 2015, at 66, 66.

19. Greene et al., *supra* note 8, at 98; *see also* Timothy H. Madden, *Data Breach Class Action Litigation – A Tough Road for Plaintiffs*, Bos. B.J., Fall 2011, at 27, 29.

20. Galbraith, *supra* note 5, at 1369.

21. 499 F.3d 629 (7th Cir. 2007).

22. 628 F.3d 1139 (9th Cir. 2010).

23. *See* discussion *infra* Section I.B.

24. 664 F.3d 38 (3d Cir. 2011),); *see* discussion *infra* Section I.B.

25. 133 S. Ct. 1138 (2013); *see* discussion *infra* Section II.A.

26. *See* discussion *infra* Section II.A.

27. *See* discussion *infra* Section II.B.

I. A Split in Approaches Toward Increased Risk Standing

As plaintiffs have turned to litigation in response to data breaches, courts have disagreed on the appropriateness of increased risk standing. This Part examines that conflict in the broader context of Article III standing principles. Section I.A outlines the requirements of and broader purposes furthered by the standing doctrine. Section I.B then considers the trajectory of data-breach cases involving increased risk standing prior to *Clapper*.

A. *Standing Principles*

Article III of the Constitution limits courts' power by allowing them to decide only actual "Cases" or "Controversies."[28] The standing doctrine defines who can bring suit for a particular claim.[29] To establish standing, a plaintiff must satisfy the burden of proof for three elements. First, a plaintiff must have suffered an injury-in-fact, defined as "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not "conjectural" or "hypothetical."'"[30] Second, the injury must have been caused by the defendant's actions.[31] Third, the injury must be likely to be redressed by a favorable decision.[32] Because courts treat Article III standing as an issue of subject-matter jurisdiction that persists through all stages of a case,[33] a court cannot reach the merits of a claim if a plaintiff fails to show any of these requirements.[34]

The Court has characterized standing as "perhaps the most important" of the Article III "limits on federal judicial power."[35] The central purpose underlying the standing doctrine is the separation of powers—the idea that the Constitution reflects the "common understanding of what activities are

28. U.S. Const. art. III, § 2.

29. Amanda Mariam McDowell, Note, *The Impact of* Clapper v. Amnesty International USA *on the Doctrine of Fear-Based Standing*, 49 Ga. L. Rev. 247, 251 (2014) (citing Erwin Chemerinsky, Constitutional Law: Principles and Policies 59 (4th ed. 2011)).

30. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (footnote omitted) (citations omitted) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

31. *Id.*

32. *Id.* at 561. The causation and redressability elements are generally secondary to the injury-in-fact analysis in cases involving increased risk of identity theft. *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–42 (9th Cir. 2010) (noting that those elements were not contested). Accordingly, this Note does not address those requirements.

33. 13B Charles Alan Wright et al., Federal Practice and Procedure § 3531.15 n.1 (3d ed. 2008).

34. *See, e.g.*, Warth v. Seldin, 422 U.S. 490, 498 (1975).

35. Allen v. Wright, 468 U.S. 737, 750 (1984), *abrogated in part by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377 (2014) (abrogating *Allen* on grounds unrelated to *Allen*'s discussion of Article III standing requirements).

appropriate to legislatures, to executives, and to courts."[36] Standing also allows courts to promote judicial efficiency by preventing frivolous lawsuits.[37] Standing principles thus do not proscribe judicial power, but rather confine it to areas in which courts have the most experience.

B. *Increased Risk in Cases Decided Before* Clapper

Standing has been a frequent concern in cases where data-breach plaintiffs have suffered an increased risk of identity theft. Yet, prior to *Clapper*, courts were unable to reach a consensus on how to treat increased risk as an injury-in-fact within the standing analysis.

The first district courts to encounter increased risk found it insufficient to create standing. *Key v. DSW Inc.*[38] and *Randolph v. ING Life Insurance & Annuity Co.*[39] demonstrate the general approach taken by those courts. *Key* involved the unauthorized taking of personal financial information of the customers of a nationwide retail outlet.[40] The customers' substantial risk of identity theft was neither actual nor imminent since the customers' pleading did not establish any risk of future misuse of their information.[41] In *Randolph*, customers of an investment company suffered an increased risk of identity theft when a laptop containing the customers' personal information was stolen from an employee's home.[42] The increased risk did not create standing because the injury was "mere speculation" of identity theft "at some unspecified point in the indefinite future."[43] Both cases thus declined to recognize increased risk standing where doing so would require the court to infer the intent of the third-party actors who stole the data and to also assume that those actors would take certain actions to harm the plaintiffs.[44]

Despite their holdings, *Key*'s and *Randolph*'s discussion of third parties' intent and actual misuse of information indicates that those elements are relevant to the imminence analysis.[45] As a result, those cases leave open the possibility that increased risk can be an injury-in-fact in some cases.

---

36. *Lujan*, 504 U.S. at 559–60; *see also Allen*, 468 U.S. at 752.

37. McDowell, *supra* note 29, at 253; *see also* Erwin Chemerinsky, Constitutional Law: Principles and Policies 60–61 (4th ed. 2011).

38. 454 F. Supp. 2d 684 (S.D. Ohio 2006).

39. 486 F. Supp. 2d 1 (D.D.C. 2007).

40. *Key*, 454 F. Supp. 2d at 685–86.

41. *See id.* at 690.

42. *Randolph*, 486 F. Supp. 2d at 3–4.

43. *Id.* at 8.

44. *See id.* at 7–8; *Key*, 454 F. Supp. 2d at 690.

45. *See Randolph*, 486 F. Supp. 2d at 7–8 ("Plaintiffs . . . do not allege that the burglar who stole the laptop did so in order to access their Information, or that their Information has actually been accessed since the laptop was stolen."); *Key*, 454 F. Supp. 2d at 690 ("Plaintiff has not alleged evidence that a third party intends to make unauthorized use of her financial information or of her identity.").

The Seventh Circuit diverged sharply from those cases in *Pisciotta v. Old National Bancorp*.[46] In that case, applicants for various bank services submitted personal information as part of their applications on the bank's website.[47] Those applicants alleged that an increased risk of identity theft incurred following a "sophisticated, intentional and malicious" intrusion into the website's hosting facility, which resulted in a breach of the applicants' information.[48] Analogizing to future harm in the medical-monitoring and environmental contexts,[49] the court broadly approved increased risk standing in data-breach cases, stating 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 court disagreed that actual misuse of the stolen information was required to constitute an injury-in-fact, as the *Key* and *Randolph* courts suggested.[51] But the court did not, at any point, identify limits on increased risk standing to ensure the future injury was sufficiently imminent.[52]

In *Krottner v. Starbucks Corp.*,[53] the Ninth Circuit supplemented *Pisciotta*'s analysis of increased risk standing. Employees of the coffee retailer suffered an increased risk of identity theft after someone stole a laptop containing the employees' personal information.[54] The court followed *Pisciotta* in recognizing the similarity of increased risk of identity theft to probabilistic injuries in medical-monitoring and environmental cases.[55] But, unlike in *Pisciotta*, the court also required that in order for the plaintiff to successfully plead increased risk as an injury-in-fact, the increased risk must be related to a "credible threat of harm"[56] that is "both real and immediate."[57] Nonetheless, even though this language might have brought *Krottner* more in line

46. 499 F.3d 629 (7th Cir. 2007).

47. *Pisciotta*, 499 F.3d at 631–32.

48. *See id.* at 632.

49. These cases involve plaintiffs who have suffered an increased risk of future injury because of, respectively, exposure to toxic substances or defective medical devices, or actions that harm the environment in some way. Isaacs, *supra* note 3, at 536, 539. I discuss the strength of both comparisons in Part III. *See* discussion *infra* Section III.A.

50. *Pisciotta*, 499 F.3d at 634 & n.3 (first citing Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (medical monitoring); then citing Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (environmental); and then citing Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (environmental)).

51. *Pisciotta*, 499 F.3d at 634 & n.2.

52. *See id.* at 634.

53. 628 F.3d 1139 (9th Cir. 2010).

54. *Krottner*, 628 F.3d at 1140–41.

55. *See id.* at 1142–43.

56. *Id.* at 1143 (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002)).

57. *Id.* at 1143 (quoting Los Angeles v. Lyons, 461 U.S. 95, 102 (1983)).

with the injury-in-fact requirement than *Pisciotta*,[58] *Krottner* failed to explain how the employees' increased risk met such a standard.[59]

Taken together, these cases suggested an entirely different approach than the one taken in *Key* and *Randolph*. But the scope of standing based on increased risk remained imprecise; although *Krottner* slightly clarified *Pisciotta*'s broad approval of increased risk standing, neither case identified clear boundaries to apply moving forward.

In *Reilly v. Ceridian Corp.*,[60] the Third Circuit split from *Pisciotta* and *Krottner* and rejected increased risk of identity theft as a basis for standing. In that case, employees of a law firm brought various claims against the firm's payroll-processing company after a hacker broke into the company's network and gained access to the employees' information.[61] The court held that the employees' increased risk of identity theft was not imminent enough, since there was no actual misuse of the stolen information.[62] In addition, the court questioned the independent value of *Pisciotta*'s and *Krottner*'s holdings given that they justified increased risk standing through analogy to other factual contexts, rather than by reference to standing principles.[63] The court also considered the analogies themselves to be substantively inadequate.[64]

Despite its clear disagreement with *Pisciotta* and *Krottner*, *Reilly* contained language that, as in *Key* and *Randolph*, indicated a willingness to find standing for some claims based on increased risk. The court pointed out that "there is no evidence that the intrusion was intentional or malicious,"[65] suggesting that different facts might have produced a different result. The court's discussion of the independent actions of third parties also revealed that the court might consider other factors relevant to assessing the imminence of the future harm.[66] Consequently, it is not clear that the split between *Reilly* and *Pisciotta* and *Krottner* is irreconcilable.

II. *Clapper*'s Effect in the Data-Breach Context

These conflicting approaches made the viability of increased risk standing unclear. The Supreme Court's subsequent consideration of increased risk standing in a separate context—in *Clapper v. Amnesty International*

58. *See supra* note 30 and accompanying text.

59. *See* 628 F.3d at 1143.

60. 664 F.3d 38 (3d Cir. 2011).

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

62. *Id.* at 44.

63. *See id.*

64. *See id.* at 44–46.

65. *Id.* at 44.

66. *See id.* at 42 (noting that realization of employees' future injuries required that a data thief have "(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 [the employees] by making unauthorized transactions in [the employees'] names").

USA[67]—only compounded the uncertainty created by the circuit split. Given *Clapper*'s factual similarity to data-breach cases, many have interpreted it to limit increased risk standing in the data-breach context.[68]

This Part asserts that *Clapper* did not eliminate the possibility of increased risk standing in data-breach cases, but instead provided a way to reconcile the preceding split. Section II.A contends that the facts in *Clapper* necessitated a stricter standing analysis such that *Clapper* did not disturb Supreme Court precedent that considers probabilistic harm an injury-in-fact. Section II.B reviews the contrasting conclusions reached by district courts applying *Clapper* in data-breach cases and uses *Clapper* to propose an interpretation that explains the inconsistent results.

A. Clapper*'s Place in the Article III Standing Framework*

Clapper examined the imminence portion of the injury-in-fact requirement in the context of a constitutional challenge to 50 U.S.C. § 1881a, a provision of the Foreign Intelligence Surveillance Act ("FISA") Amendments Act of 2008.[69] Section 1881a allowed the United States to conduct foreign intelligence surveillance without having to fulfill certain requirements associated with traditional FISA surveillance.[70] The plaintiffs were attorneys and organizations that frequently exchanged confidential information with clients abroad who might be targeted under Section 1881a.[71] Consequently, the plaintiffs claimed that Section 1881a created an "objectively reasonable likelihood" of injury through the acquisition of their communications under Section 1881a–sanctioned surveillance.[72] The plaintiffs also argued that the risk of Section 1881a surveillance caused a present injury because such risk necessitated that they incur costs to protect the confidentiality of their communications.[73]

In rejecting both theories of standing, *Clapper*'s discussion of the imminence standard appeared to set a high bar for other injuries based on increased risk. The Court noted that the central purpose of the imminence

67. 133 S. Ct. 1138 (2013).

68. *See* discussion *infra* Section II.B.1 *See generally* John L. Jacobus & Benjamin B. Watson, Clapper v. Amnesty International *and Data Privacy Litigation: Is a Change to the Law "Certainly Impending?"*, 21 RICH. J.L. & TECH. 3 (2014), http://jolt.richmond.edu/v21i1/article3.pdf [perma.cc/E2ST-EPB7] (examining potential impact of *Clapper*'s holding on data-breach cases).

69. *See Clapper*, 133 S. Ct. at 1144.

70. *See id.*

71. *Id.* at 1145.

72. *See id.* at 1146.

73. *Id.* This type of injury is a common counterpart to increased risk of future harm in data-breach cases. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (collecting cases in which costs to mitigate increased risk of future injury were analyzed as separate injury).

requirement is to ensure that the alleged future injury is "*certainly* impending,"[74] and it stressed that allegations of "*possible* future injury" were insufficient to confer standing.[75] The Court rejected the Second Circuit's "objectively reasonable likelihood" standard as inconsistent with these requirements.[76] The Court then repeated the "certainly impending" phrase several times over the course of its brief discussion of increased risk,[77] concluding that the plaintiffs had failed to show that the future harm was imminent.[78] The Court reached a similar conclusion regarding the plaintiffs' incurred mitigation costs, holding that whether this type of harm is an injury depends largely on the initial determination as to the imminence of the future injury itself.[79]

Some have speculated that the Court's emphasis of "certainly impending" signaled a departure from standing precedent. As Justice Breyer argued in his dissent, the Court's focus on the certainty of the future harm may demand too much of a plaintiff, given the inherent uncertainty of the future.[80] Indeed, a literal reading of "certainly impending" would preclude almost any claim based on fear of future injury, given the guesswork involved in predicting future events.[81] Even apart from this literal interpretation, it is possible to understand *Clapper* as simply rejecting an "objectively reasonable likelihood" standard.[82] This reading would still leave little room to find standing where a plaintiff could only show a minor increase in the risk of future harm.[83] Both interpretations would limit a plaintiff's ability to bring a claim without any present injury.

Clapper's understanding of the nature of imminence in the standing context thus seems inconsistent with previous cases in which plaintiffs established standing based on increased risk. The Supreme Court has frequently found standing where future injury was not certain, and it has used language

74. *Clapper*, 133 S. Ct. at 1147 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 565 n.2 (1992)).

75. *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

76. *Id.*

77. *See id.* at 1147–50.

78. *Id.* at 1150.

79. *See id.* at 1151 (citing Pennsylvania v. New Jersey, 426 U.S. 660, 664 (1976), and Nat'l Family Planning & Reprod. Health Ass'n, Inc. v. Gonzales, 468 F.3d 826, 831 (C.A.D.C. 2006)) ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."). Some courts have applied this same logic in the data-breach context. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657–58 (S.D. Ohio 2014). As discussed in Section III.B below, mitigation costs might be the only injury that can qualify as cognizable injury. Accordingly, an appropriate standing analysis for data-breach cases should ensure that such costs were incurred based upon imminent harm.

80. *See Clapper*, 133 S. Ct. at 1160–61 (Breyer, J., dissenting).

81. McDowell, *supra* note 29, at 266.

82. *See Clapper*, 133 S. Ct. at 1147.

83. Jacobus & Watson, *supra* note 68, ¶ 102.

suggesting a less restrictive standard than "certainly impending."[84] In *Monsanto Co. v. Geertson Seed Farms*,[85] for instance, farms that produced conventional alfalfa seeds challenged the government's decision to cease regulating a certain type of genetically engineered alfalfa crop.[86] Those farms asserted standing on the basis that their conventional alfalfa crops would be infected with the genetically engineered gene if the deregulation were permitted, damaging the farms' business.[87] The Court found standing based on the "*substantial risk* of gene flow" caused by the deregulation.[88] Likewise, in *Davis v. FEC*,[89] a self-financed candidate for the House of Representatives had standing to challenge the constitutionality of a statute regulating campaign contributions where he faced a "*realistic* and *impending* threat of direct injury" from the operation of the statute, without demonstrating that such future harm would definitely occur.[90] Other cases have employed similar phrases to describe a plaintiff's satisfaction of the imminence requirement,[91] all of which are more lenient than "certainly impending." *Clapper* did not overrule any of these prior holdings.[92] Nonetheless, the Court's preference for the "certainly impending" standard might reflect an implicit adoption of that phrase as the appropriate standard for judging the imminence of probabilistic harm.

Yet a closer reading of *Clapper* indicates that it comports with the Court's precedent regarding increased risk. Two key factors lessen the impact of the "certainly impending" standard.

First, a stricter standing analysis was particularly appropriate in *Clapper*. The Court faced a constitutional challenge to a statute passed by Congress, and that situation demanded a closer standing inquiry than in other cases.[93] National security concerns involved in *Clapper* may also have necessitated its closer inquiry.[94] Finally, the plaintiffs' fear that future harm would ever occur was "highly speculative," as it relied on a "highly attenuated chain of

84. *Clapper*, 133 S. Ct. at 1160–61 (Breyer, J., dissenting).

85. 561 U.S. 139 (2010).

86. *Monsanto*, 561 U.S. at 146.

87. *See id.* at 153–54.

88. *Id.* at 153 (emphasis added). The Court also cited with approval the district court's discussion of the "reasonable probability" of gene flow, *see id.*, an even lower standard than "substantial risk."

89. 554 U.S. 724 (2008).

90. *Davis*, 554 U.S. at 734–35 (interpreting Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979)) (emphasis added).

91. *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2343 (2014) ("credible threat of enforcement"); Dep't of Commerce v. U.S. House of Representatives, 525 U.S. 316, 333 (1999) ("substantially likely" to suffer future injury); Clinton v. New York, 524 U.S. 417, 432 (1998) ("sufficient likelihood of economic injury"); Pennell v. City of San Jose, 485 U.S. 1, 8 (1988) ("realistic danger of . . . direct injury" (quoting *Babbitt*, 442 U.S. at 298)).

92. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

93. *See id.* at 1147.

94. *See* Jacobus & Watson, *supra* note 68, ¶ 100 (citing Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014)); Scott Michelman, *Who Can*

possibilities."[95] The standing analysis is more exacting when the future injury depends on an independent decisionmaker, particularly a court, exercising its discretion in a certain way.[96] That concern was amplified in *Clapper*, where the realization of the plaintiffs' speculative chain would have required multiple actors, including the Foreign Intelligence Surveillance Court, to make certain decisions that would eventually lead to the government acquiring the plaintiffs' communications.[97] The presence of all three case-specific factors likely led the Court to apply a more stringent standard regarding future harm, making the use of the "certainly impending" standard less indicative of a precedential shift.

Second, *Clapper*'s discussion of the applicable standard for the imminence requirement reduces the significance of the Court's repetition of the "certainly impending" standard. The Court acknowledged that "imminence is . . . a somewhat elastic concept."[98] Perhaps in recognition of this flexibility, the Court conceded in a footnote that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about."[99] The Court then acknowledged the existence of the previously recognized "substantial risk" standard for increased risk of future harm.[100] Although authors have consistently recognized that this footnote validates both the "certainly impending" and "substantial risk" standards,[101] they disagree on the preferred resolution of these coexisting standards.[102] The Court did not offer guidance in the footnote; indeed, the Court left open the possibility that the two standards are functionally identical.[103] But, regardless of the exact situations in which each standard should be used, the Court's discussion suggests that the "certainly impending" standard was not intended to entirely displace previous standards that were more likely to

---

Sue Over Government Surveillance?, 57 UCLA L. Rev. 71, 71 (2009) ("In some cases, courts impose on surveillance plaintiffs a stricter test for probabilistic injuries than exists in the rest of standing law . . . ."). The Court itself noted the national security concerns present in the case. *See Clapper*, 133 S. Ct. at 1147 ("[W]e have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs."). For an argument that *Clapper* should nevertheless be read to apply broadly beyond the surveillance context, see McDowell, *supra* note 29, at 270–72.

95. *Clapper*, 133 S. Ct. at 1148.

96. *See id.* at 1150; *see also* Whitmore v. Arkansas, 495 U.S. 149, 157, 159 (1990).

97. *See Clapper*, 133 S. Ct. at 1148–50.

98. *Id.* at 1147 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 565 n.2 (1992)).

99. *Id.* at 1150 n.5.

100. *See id.* (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–54 (2010)).

101. *See* Jacobus & Watson, *supra* note 68, ¶ 101; McDowell, *supra* note 29, at 273; Andrew C. Sand, Note, *Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in* Clapper v. Amnesty International USA, 113 Mich. L. Rev. 711, 731 (2015).

102. *Compare* McDowell, *supra* note 29, at 274–79, *with* Sand, *supra* note 101, at 732.

103. *See Clapper*, 133 S. Ct. at 1150 n.5.

permit standing based on increased risk of future harm.[104] Rather, the Court needed to adapt its standards to address particular facts that demanded a stricter standing analysis.[105] Consequently, *Clapper* did not alter the standing framework but only supplemented that framework in a narrow manner.

B. *District Courts' Conflicting Interpretations of* Clapper

Following the Court's own uncertainty in *Clapper* as to the appropriate imminence standard, a number of district courts have reached contrasting conclusions regarding the viability of standing based on increased risk in data-breach cases.[106] Examining these conflicting applications of *Clapper* reveals a possible reconciliation of the two district court camps based on the nature of the data breaches at issue in the cases.[107] This interpretation permits increased risk to serve as an injury-in-fact, consistent with *Pisciotta* and *Krottner*.

1. Courts Adopting *Clapper*'s Stricter Standard

The majority of district courts considering standing in the data-breach context have declined to find standing based on an increased risk of identity theft, considering *Clapper*'s "certainly impending" standard determinative. In *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*,[108] for example, a thief stole data tapes containing personal information and medical records for 4.7 million members of the U.S. military and their families, who were enrolled in a health care program that contracted with the defendant, an information technology company, to protect such information.[109] The court concluded that the enrollees' increased risk of identity theft and mitigation costs were not injuries-in-fact because the increased risk did not qualify as "certainly impending" under *Clapper*.[110] As in *Clapper*, the dependence of the future injury on a third party's actions made those injuries nonimminent.[111] The court also suggested that those data-breach cases permitting standing based on increased risk of harm, including *Pisciotta* and *Krottner*, were no longer viable in light of *Clapper*.[112]

---

104. *See* McDowell, *supra* note 29, at 273 ("*Clapper* is best read as only a slight shift to a stricter standing doctrine and . . . not . . . as a major departure from current standing jurisprudence.").

105. *See supra* notes 93–97 and accompanying text.

106. *See* discussion *infra* Sections II.B.1 & II.B.2.

107. *See* discussion *infra* Section II.B.3.

108. 45 F. Supp. 3d 14 (D.D.C. 2014).

109. *Sci. Applications Int'l Corp*, 45 F. Supp. 3d at 19.

110. *See id.* at 25–26.

111. *See id.* at 25.

112. *See id.* at 27–28.

Other cases have gone even further in arguing that the standard imposed by *Clapper* precludes a more permissive approach to standing. *Strautins v. Trustwave Holdings, Inc.*[113] used *Clapper* to constrain the scope of *Pisciotta*. Individuals who had filed tax returns with the state department of revenue lacked standing to bring claims against the data-security company that provided services for that department following a cyberattack, where the injuries related solely to an increased risk that those individuals' personal information would be misused.[114] Recognizing that *Pisciotta* "contain[ed] no language describing the degree of risk exposure required to confer standing," the court reasoned that that case "leaves open by implication the argument that *any* degree of risk enhancement could suffice" to show standing.[115] The court deemed this low bar to be at odds with the high "threshold of probability" required by *Clapper* for future injuries.[116]

Similarly, in *Peters v. St. Joseph Services Corp.*,[117] a hospital patient alleged that she had suffered an increased risk of identity theft as a result of the potential acquisition of her personal information by hackers who infiltrated the hospital's computer network.[118] The court rejected the future injury as too speculative given the number of intervening acts necessary to cause such harm.[119] The court further noted the difference between a mere increase in risk of future harm and the level of risk required to satisfy the "certainly impending" or "substantial risk" standards.[120] As a result, the court observed, *Clapper* resolved the circuit split between *Pisciotta*, *Krottner*, and *Reilly*.[121] As with the preceding cases, *Peters* thus provides a strong basis for rejecting *Pisciotta*'s and *Krottner*'s approval of increased risk standing, since those cases did not clearly identify the degree of risk required to satisfy the injury-in-fact requirement.[122]

2. Courts Rejecting *Clapper*'s Effect

A number of district courts, however, have declined to find that *Clapper* affected the precedential strength of either *Pisciotta* or *Krottner*. *Moyer v. Michaels Stores, Inc.*[123] held that *Clapper* had not displaced *Pisciotta*. Customers of an arts-and-crafts retailer alleged that, because their credit or debit

113. 27 F. Supp. 3d 871 (N.D. Ill. 2014).

114. *See Strautins*, 27 F. Supp. 3d at 873, 875.

115. *Id.* at 878.

116. *Id.*

117. 74 F. Supp. 3d 847 (S.D. Tex. 2015).

118. *See Peters*, 74 F. Supp. 3d at 850–51.

119. *See id.* at 854.

120. *Id.* at 855.

121. *Id.* at 856.

122. *See supra* notes 52, 59 and accompanying text.

123. No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).

card information was exposed during a data breach announced by the retailer, they had suffered an increased risk of identity theft.[124] The court held that, consistent with *Pisciotta*, an increased risk of identity theft could still be an injury-in-fact after *Clapper*.[125] *Moyer* recognized that *Clapper* represents a single case in a framework of cases that collectively define the boundaries of Article III standing.[126] Consequently, *Clapper* did not undermine *Pisciotta*'s precedential value as to standing in data-breach cases.

Two cases reaffirmed the strength of *Krottner* post-*Clapper*. First, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[127] the defendant network requested that, in light of *Clapper*, the court reconsider its previous ruling that the plaintiff users' increased risk of identity theft constituted an injury-in-fact under *Krottner*.[128] The court rejected the network's contention that *Clapper* "tightened the 'injury-in-fact' analysis" in *Krottner*, concluding that the standard used to evaluate imminence in *Clapper* was only semantically—not substantively—distinct from its counterpart in *Krottner*.[129] *Clapper* "simply reiterated an already well-established framework for assessing" imminence.[130] That conclusion is consistent with the approach in cases regarding probabilistic harm that preceded *Clapper*, which used various phrases to recognize increased risk as imminent enough to be considered an injury-in-fact.[131]

Likewise, in *In re Adobe Systems, Inc. Privacy Litigation*,[132] subscribers to the defendant's licensed products suffered an increased risk of future harm when their personal information was acquired by hackers who gained access to the defendant's servers and spent several weeks decrypting and removing that information from the network.[133] The court first noted that *Clapper* existed comfortably within the Article III standing framework.[134] Moreover, the underlying similarity between the imminence standards used in both cases led the court to conclude that *Clapper* did not overrule *Krottner*.[135] The court also highlighted the relative likelihood that the plaintiffs' information

124. *Moyer*, 2014 WL 3511500, at *1, *4.

125. *Id.* at *5.

126. *See id.* ("The labels used to describe the imminence requirement in [certain Supreme Court] cases . . . sound less demanding than *Clapper*'s rigorous application of the 'certainly impending' standard.") (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013)).

127. 996 F. Supp. 2d 942 (S.D. Cal. 2014).

128. *Sony Gaming*, 996 F. Supp. 2d at 960; *see also In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 958 (S.D. Cal. 2012).

129. *See Sony Gaming*, 996 F. Supp. 2d at 961 (quoting Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Circ. 2010)).

130. *Id.*

131. *See supra* notes 84–92 and accompanying text.

132. 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

133. *See Adobe Systems*, 66 F. Supp. 3d at 1206–07.

134. *See id.* at 1213–14 ("In the absence of any indication in *Clapper* that the Supreme Court intended a wide-reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper* represents the sea change that [defendant] suggests.").

135. *See id.* at 1214.

would be misused, compared to the highly attenuated chain of possibilities in *Clapper*.[136] On its face, then, *Adobe*—as well as *Sony Gaming* and *Moyer*—rejected the dominant trend and preserved a place for increased risk in the data-breach context.

3. Resolution of Conflicting Approaches

The standing analyses of the cases discussed above are, at first glance, troubling. Whether data-breach plaintiffs can bring claims based on an increased risk of future harm in a particular court depends largely upon the standing approach adopted by the federal circuit in which plaintiffs bring their claims—a question of geographic coincidence.[137] Moreover, the continued divergence of district courts regarding data-breach standing suggests that *Clapper* has done little, if anything, to resolve the split arising from *Pisciotta*, *Krottner*, and *Reilly*.[138]

Despite this apparent impasse, the varying treatment of increased risk of harm from data breaches may be resolvable, with *Clapper* providing a starting point. Even if *Clapper* did not entirely supplant the more lenient standing framework used in prior cases,[139] the Court's rejection of an "objectively reasonable likelihood" standard nevertheless changed the standing framework by significantly impeding claims based on minimal or normal risks of future harm.[140] Given this narrower framework, the standing inquiry in data-breach cases must be strict enough to weed out those plaintiffs whose future injuries are not imminent enough to satisfy even the "substantial risk" standard, yet are broad enough to permit the claims of those plaintiffs who have a well-founded concern of imminent future injury.

Viewed from this perspective, *Clapper* does not preclude all data-breach claims based on increased risk of identity theft—only those based on future harm that is not imminent.[141] The disparate conclusions reached in the circuit and district courts, both before and after *Clapper*, therefore do not reflect complete disagreement as to the legitimacy of increased risk standing in data-breach cases. Instead, those incongruous holdings indicate courts' uneven attempts to identify what constitutes imminent risk of identity theft.

---

136. *See id.* at 1214–16.

137. At least one author has suggested, in a different context, that the articulation by different circuits of conflicting standards regarding standing may create forum-shopping problems. Peter S. Massaro, III, Note, *Filtering Through a Mess: A Proposal to Reduce the Confusion Surrounding the Requirements for Standing in False Advertising Claims Brought Under Section 43(a) of the Lanham Act*, 65 WASH. & LEE L. REV. 1673, 1699 (2008).

138. *See* J. Thomas Richie, ABA, *Data Breach Class Actions*, BUS. LITIG. COMMITTEE NEWS, (ABA Tort Trial and Insurance Practice Section, Chicago, IL), Winter 2015, at 1, 10, http://www.americanbar.org/content/dam/aba/uncategorized/tips/blc/2015BusinessLitigationWinter.authcheckdam.pdf [http://perma.cc/7G4U-M4GG].

139. *See supra* Section II.A.

140. *See* Jacobus & Watson, *supra* note 68, ¶ 102; McDowell, *supra* note 29, at 274.

141. Indeed, *Strautins* conceded this point. *See* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 (N.D. Ill. 2014) ("*Clapper* does not completely close the door on probabilistic harm as a basis for standing . . . .").

The factual differences between the cases on both sides of the split illustrate the fact-specific nature of the imminence inquiry and, in turn, illustrate that cases based on increased risk of identity theft can be compatible with *Clapper*. In almost all of the cases that rejected injuries-in-fact based on increased risk of future harm, the details of the breach were uncertain, as it was unclear whether the hacker or thief was even able to access the stolen data.[142] By contrast, the cases that reached the opposite conclusion regarding standing based on increased risk involved deliberate, targeted hacks,[143] thefts of unprotected information,[144] or attempted fraudulent activity following the data breach.[145] The presence of at least one of those factors indicates that the stolen data is much more likely to be misused, as compared to a normal data breach.[146] Accordingly, injuries based on some combination of the factors are sufficiently imminent to qualify as injuries-in-fact even after *Clapper*, since such facts would cause the risk of identity theft to meet the applicable "substantial risk" or "certainly impending" standard.

III. Problems with Identifying an Appropriate Standing Framework

This discussion illustrates that an increased risk of identity theft can create standing in certain circumstances, even if those circumstances are narrow. One option, given this limitation, is to determine the imminence of increased risk using a more individualized approach relying on certain indicative factors.[147] Yet the Seventh and Ninth Circuits—the only circuits to have endorsed standing based on increased risk—found standing in *Pisciotta*

142. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 850 (S.D. Tex. 2015); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *Strautins*, 27 F. Supp. 3d at 875; *In re* Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *1–2 (N.D. Ill. Sept. 3, 2013).

143. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632, 634 (7th Cir. 2007) ("[T]he scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious."); *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (describing intentional and thorough nature of hacking incident); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 955 (S.D. Cal. 2014) (detailing scope of hack).

144. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (pointing out that data on stolen laptop was unencrypted).

145. *See id.* at 1141 (noting attempted misuse of plaintiff's social security number); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *1 (N.D. Ill. July 14, 2014) (stating that defendant's press release regarding breach was prompted by possible fraudulent activity on some customers' payment cards).

146. *See Fact Sheet 17: Coping with Identity Theft: Reducing the Risk of Fraud*, Privacy Rts. Clearinghouse, https://www.privacyrights.org/fs/fs17-it.htm [https://perma.cc/ZUK2-EXHM] (recommending increased password security to protect against identity theft, especially where data theft was intentional and targeted).

147. *See* discussion *supra* Section II.B.3.

and *Krottner* not because of specific case-related facts, but instead, by analogy to other types of future harm.[148]

This Part rejects the approaches for analyzing standing based on increased risk of identity theft used in *Pisciotta* and *Krottner*, and it considers another hurdle that any increased risk standing framework must take into account. Section III.A evaluates the comparisons to increased risk in medical-monitoring and environmental cases and concludes that factual dissimilarities limit the value of these analogies. Section III.B identifies an additional problem related to pleading damages for increased risk that qualifies as an injury-in-fact, and it argues that a workable standing framework for increased risk must account for this challenge.

A. *Comparison to Medical-Monitoring and Environmental Cases*

Both *Pisciotta* and *Krottner* looked to medical-monitoring and environmental cases to guide their interpretations of increased risk as an injury-in-fact.[149] But the facial similarities between the injuries in those cases and data-breach cases only obscure fundamental differences, making those cases poor points of comparison for future harm in the data-breach context.

Medical-monitoring cases involve presently healthy plaintiffs who have suffered an increased risk of future harm,[150] either by using a defective medical device or prescription drug[151] or by being exposed to a toxic substance.[152] Like plaintiffs in data-breach cases, plaintiffs in medical-monitoring cases have not actually endured any harm when they bring suit, but might suffer an injury at some point in the future.[153] That risk gives rise to compensable harm based on the costs of medical monitoring to prevent the injury from occurring.[154] Similarly, environmental cases involve a plaintiff's inability to

148. *See supra* notes 50, 56 and accompanying text.

149. *See Krottner*, 628 F.3d at 1142–43; Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 & n.3 (7th Cir. 2007).

150. *E.g.*, Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 571 (6th Cir. 2005).

151. *See, e.g.*, *id.* at 573–74; Bouldry v. C.R. Bard, Inc., 909 F. Supp. 2d 1371, 1375–76 (S.D. Fla. 2012); *In re* Propulsid Prods. Liab. Litig., 208 F.R.D. 133, 139 (E.D. La. 2002).

152. *See, e.g.*, Duke Power Co. v. Carolina Envtl. Study Grp., Inc., 438 U.S. 59, 74 (1978); *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 850 (3d Cir. 1990).

153. *See Sutton*, 419 F.3d at 573–74.

154. *Paoli*, 916 F.2d at 850–51. Although *Paoli* frames the future harm and the medical-monitoring costs as separate injuries that are related to different causes of action, *see id.*, it makes more sense to consider the increased risk of future harm to be the underlying injury in both cases. *Sutton*, 419 F.3d at 572. *Clapper*'s conclusion that future harm and present costs incurred are inextricably linked only reinforces this view. *See supra* note 79 and accompanying text.

enjoy an area she normally uses,[155] or an increased risk that some activity affecting the environment will injure the plaintiff in the future.[156]

Pisciotta and *Krottner* both found these rationales compelling as applied to data-breach cases,[157] but neither case examined the specific logic underlying medical-monitoring and environmental cases. One author has sought to fill in these gaps. As to medical-monitoring cases, Miles Galbraith argues that the medical-monitoring remedy "perfectly parallels the costs incurred by plaintiffs in data breach cases for credit-monitoring services: like periodic tests to evaluate the health of their body, credit monitoring serves to ensure the financial health of the plaintiffs."[158] Galbraith bases this conclusion on *Paoli*'s distinction between future harm and medical-monitoring costs, asserting that "credit-monitoring costs are distinguishable from whatever harm may occur in the future as a result of identity theft."[159] Galbraith further contends that credit monitoring serves as a "[p]rophylactic measure[ ]" to protect against more significant consequences of identity theft in the same way that medical monitoring prevents future physical injury.[160] As to environmental cases, Galbraith asserts that they are reliable guides for future harm in data-breach cases because environmental cases show a "willingness in courts to permit plaintiffs to sustain a claim for an increased risk of future harm."[161]

These arguments, however, ignore the dissimilarities between the injuries underlying the claims in each case. In medical-monitoring cases, "an injury has undoubtedly occurred," and "the damage has been done; we just cannot yet quantify how it will manifest itself."[162] Similarly, future injuries in environmental cases are direct consequences of a defendant's actions,[163] so the harm has, in some sense, already occurred at the time of suit. Credit monitoring, in contrast, protects against fraudulent activity that is "a harm but not a symptom of a previous injury,"[164] since identity theft necessarily

155. *E.g.*, Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 183 (2000).

156. *See, e.g.*, Cent. Delta Water Agency v. United States, 306 F.3d 938, 948 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000); Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir. 1993).

157. *See supra* note 149 and accompanying text.

158. Galbraith, *supra* note 5, at 1392.

159. *Id.* at 1391.

160. *Id.* at 1392. Such effects could include "financial ruin [or] the inability to get credit or obtain employment." *Id.* at 1393 n.197 (citing Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 Geo. Mason L. Rev. 113, 130 (2011)).

161. Galbraith, *supra* note 5, at 1396.

162. Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011).

163. Isaacs, *supra* note 3, at 539; *see also* sources cited *supra* note 156.

164. Isaacs, *supra* note 3, at 537.

requires fraud by a third party that, while related to the data breach, is distinct and separate from it.[165] Medical-monitoring and environmental claims thus seek to remedy both future *and* past harms. Credit-monitoring costs, on the other hand, only look forward to an uncertain future injury.

In addition, the future injuries in medical-monitoring and environmental cases deserve greater judicial protection than the future economic injuries in data-breach cases. Requiring less than an actual injury in medical-monitoring cases is sensible, since "'[w]aiting for a plaintiff to suffer physical injury before allowing any redress whatsoever is both overly harsh and economically inefficient.'"[166] Medical monitoring can provide vital protection against irreparable physical consequences, including death,[167] justifying finding standing before those consequences have actually occurred. Likewise, monetary compensation may not suffice to return a plaintiff to his original position in environmental cases, given the abstract nature of the future injuries,[168] so declining to find standing before the injury occurs accomplishes little.

These circumstances are not present in the context of an increased risk of identity theft. Although identity theft can have significant effects, any resulting costs are confined to the economic sector and are thus remediable in a way that physical or abstract environmental injuries are not.[169] A plaintiff could thus bring any claim if and when identity theft actually occurs. Claims based on credit-monitoring costs are therefore different from medical-monitoring and environmental claims in both kind and degree; credit-monitoring claims involve different types of injury and provide less-substantial protection than medical-monitoring and environmental claims.

Limiting *Pisciotta*'s and *Krottner*'s reliance on their comparison to medical-monitoring and environmental cases has significant doctrinal consequences. Since those cases permit a more relaxed standing analysis in certain specific contexts,[170] *Pisciotta* and *Krottner* might have intended to create a similarly broad standard for increased risk of identity theft.[171] But *Pisciotta* and *Krottner* cannot rely on the reasoning of the medical-monitoring and environmental cases to sidestep a closer standing analysis. In light of these differences, a standing inquiry emerging from *Pisciotta* and *Krottner* must be strict enough to satisfy at least the "substantial risk" test identified by the Court in *Clapper*.[172]

---

165. *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (noting that future identity theft depended on third party's fraudulent actions).

166. *Reilly*, 664 F.3d at 45 (quoting Sutton v. St. Judge Med. S.C., Inc., 419 F.3d 568, 575 (6th Cir. 2005)).

167. *See* Isaacs, *supra* note 3, at 538.

168. *Reilly*, 664 F.3d at 45; Isaacs, *supra* note 3, at 539–40.

169. *See* Isaacs, *supra* note 3, at 537–38.

170. *See supra* notes 166, 168 and accompanying text.

171. *See Reilly*, 664 F.3d at 44.

172. *See* discussion *supra* Section II.B.3.

B. *Damages-Related Limitation*

That standing inquiry must also account for data-breach plaintiffs' difficulty in pleading cognizable injury after establishing standing. As currently applied, the increased risk standing analysis frequently gives plaintiffs standing to pursue claims that are likely to be dismissed on the merits absent cognizable injuries.[173] Data-breach plaintiffs typically bring common law claims, including negligence, breach of implied contract, breach of implied warranty, or breach of fiduciary duty.[174] But even if a plaintiff has standing to pursue such claims, he must also be able to establish the prima facie elements of that claim, including cognizable injury.[175] Showing this last factor involves more than a perfunctory reapplication of the injury-in-fact analysis. Indeed, although the harms alleged are the same for both standing and cognizable injury purposes, a slightly higher burden exists to show damages.[176]

This increased burden has caused problems in the data-breach context: the damages requirement has "proven [the most] elusive" to data-breach plaintiffs.[177] Courts have consistently rejected common law claims where plaintiffs could not allege a compensable injury related to increased risk of identity theft.[178] Courts have also declined to recognize credit-monitoring costs as a cognizable injury in negligence cases given that the economic-loss rule theoretically bars recovery of purely economic losses through tort claims.[179] Certainly, courts should continue to conduct the damages and standing inquiries separately so that the standing analysis retains its independent value in the judicial process.[180] Yet, if increased risk claims can be so easily dismissed where standing is satisfied, then that standing analysis has only nominal value.

Despite these apparent barriers, courts have not foreclosed the possibility that increased risk of identity theft could result in cognizable injury. Courts have acknowledged the possibility that credit-monitoring costs may

173. *See infra* note 178 and accompanying text.

174. Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 Ala. L. Rev. 395, 405 (2014).

175. Isaacs, *supra* note 3, at 543–44; *see also* Cease, *supra* note 174, at 405.

176. Galbraith, *supra* note 5, at 1397; *see also* Patricia Cave, Comment, *Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 Cath. U. L. Rev. 765, 778 (2013).

177. Douglas H. Meal & David T. Cohen, *Private Data Security Breach Litigation in the United States*, *in* Privacy and Surveillance Legal Issues 101 (2014), 2014 Westlaw 10442.

178. *See, e.g.*, Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639–40 (7th Cir. 2007); Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014).

179. *See* Galbraith, *supra* note 5, at 1396 & n.226. *But see* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 Geo. Mason L. Rev. 113, 122–23 (2011) ("The . . . 'economic loss rule' does not bar recovery of credit-monitoring losses.").

180. *See* Galbraith, *supra* note 5, at 1397–98 (arguing conflation of standing and cognizable injury analyses prevents plaintiffs from proceeding with legitimate claims).

qualify as damages, just as mitigation costs can in medical-monitoring cases.[181] This approach depends on whether a state recognizes a different damages test for medical-monitoring claims, which is unsettled.[182] But it is a preferable alternative to considering credit-monitoring costs on their own terms, since courts not relying on this comparison have either rejected credit-monitoring damages as injuries[183] or required actual or attempted theft prior to the purchase of credit monitoring.[184] Consequently, the medical-monitoring analogy provides a useful starting point for an appropriate standing framework that has independent value, since that approach narrows the range of acceptable claims based on increased risk without preventing them altogether.

IV. Proposed Standing Framework

The complications identified in Part III demonstrate that an improvement to the data-breach standing analysis is necessary. Maintaining the law as it is currently applied would harm consumers.[185] A straightforward Article III standing analysis is practically flawed for two reasons. First, that framework produces inconsistent results depending on the court.[186] Second, it frequently recognizes standing to pursue claims that, lacking compensable injuries, are likely to be dismissed.[187] This latter barrier prevents successful recovery for legitimate injuries-in-fact.

This Part suggests an alternative framework that accounts for both of these problems. Section IV.A proposes a stricter, factor-based standing analysis of increased risk that merges elements from the standing and damages inquiries. Section IV.B considers whether to apply this framework through legislative or judicial means. The Section concludes that judicial implementation will preserve the ability to bring claims involving cognizable injury while avoiding speculative increased risk claims that would likely result from legislative solutions.

---

181. *See, e.g.*, *Sony Gaming*, 996 F. Supp. 2d at 970; Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281–82 (S.D.N.Y. 2008). It might seem inconsistent to endorse a comparison to medical-monitoring cases in this context while rejecting the same comparison in another. But the analogy here depends on structural similarities between the monitoring and the harm in each case, *see* Johnson, *supra* note 179, at 132–39, whereas the standing comparison depended on substantive similarities between the harm suffered in each case. *See* discussion *supra* Section III.A.

182. *See Pisciotta*, 499 F.3d at 639; Johnson, *supra* note 179, at 132 n.129 (collecting cases reaching conflicting conclusions).

183. *See Moyer*, 2014 WL 3511500, at *7 (first citing Williams v. Manchester, 888 N.E.2d 1, 13 (Ill. 2008); and then citing Worix v. MedAssets, Inc., 857 F. Supp. 2d 699, 704–05 (N.D. Ill. 2012)).

184. *See* Cave, *supra* note 176, at 779; *see also* Anderson v. Hannaford Bros. Co., 659 F.3d 151, 166 (1st Cir. 2011).

185. Cave, *supra* note 176, at 786.

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

187. *See* discussion *supra* Section III.B.

A. *Factor-Based Framework*

An ideal framework would rely in part on *Clapper*'s interpretation of the injury-in-fact requirement. Courts' application of *Clapper* in the data-breach context has revealed the importance of certain facts in establishing the imminence of identity theft, including the intent of the data thief, the protection of the data, and the attempted misuse of the stolen data.[188] The framework thus must require plaintiffs to show the presence of these factors to some degree.

But the standing analysis should also anticipate the damages inquiry to prevent the otherwise-inevitable dismissal of claims. An appropriate framework, alluded to by a district court considering increased risk standing in *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*,[189] could borrow from the medical-monitoring damages analogy and require a plaintiff to also show that she incurred credit-monitoring costs because she had a rational basis for fearing that her data would be misused.[190] Courts would have to individually evaluate the rationality of a plaintiff's fear based on several factors, including:

> (1) the of lack [sic] any password-protection for use of the computer such that an unsophisticated user could boot the computer and immediately access the file; (2) that the person stealing the hard drive was motivated by a desire to access the data and had the capabilities to do so; or (3) actual access or misuse of information of the plaintiff or another person whose data was stored on the same hard drive.[191]

These factors would impose a greater burden on the plaintiff to demonstrate a reasonable fear of future injury at an earlier stage. This mixing of the standing and damages tests is appropriate here given the similar factors involved in each inquiry, and the reality that "consideration of injury for standing purposes inherently implicates weighing the merits of the claim."[192] Adopting a form of the *Caudle* framework at the standing stage would also increase the likelihood of success after establishing standing, since plaintiffs who meet this stricter test would be well-positioned to have their credit-monitoring costs qualify as compensable injuries.

---

188. *See* discussion *supra* Section II.B.3; *see also supra* note 66 (outlining factors discussed in *Reilly v. Ceridian Corp.* to make alleged injury imminent). One author has identified *Reilly*'s factors as reflecting the Third Circuit's standing requirements. *See* Isaacs, *supra* note 3, at 555. But *Reilly* did not indicate that every data-breach plaintiff *must* show these facts to establish standing; it observed only the conditions necessary for plaintiffs' future injuries to occur. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011). Nonetheless, I agree with Isaacs that those factors are important given their similarity to the common factors I have identified above.

189. 580 F. Supp. 2d 273 (S.D.N.Y. 2008).

190. *Caudle*, 580 F. Supp. 2d at 282.

191. *Id.*

192. Cave, *supra* note 176, at 787 (footnote omitted); *see also* William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 238–39 (1988) (discussing ways in which "standing determinations are actually determinations on the merits").

B. *Preferred Method of Implementation*

Nonetheless, this standing analysis lacks value if not appropriately implemented. Solutions will likely come from either judicial or legislative action.[193] Several authors who have examined the fractured state of increased risk standing, including Patricia Cave and Elizabeth Isaacs, have endorsed the passage of a federal statute creating a private right of action establishing standing for increased risk of identity theft.[194] Cave's and Isaacs's frameworks—the two most detailed proposals—are largely similar: both envision a broader role for the Federal Trade Commission in establishing and enforcing data management standards,[195] and both identify credit-monitoring expenses as the only recoverable damages.[196] But Isaacs clarifies the ambiguities of Cave's outline by suggesting both reliance on the *Reilly* factors[197] to narrow the types of data breaches for which a private right of action is available,[198] and limiting recovery to actual, reasonable costs for credit monitoring.[199]

The benefits of these statutory solutions are clear. The existence of clear federal guidelines would better standardize businesses' data privacy practices, and the existence of statutory remedies would incentivize compliance.[200] In addition, federal legislation could replace the gaps that plague states' approaches to damages for increased risk of identity theft, and it would resolve the inconsistencies as to standing inquiries in data-breach cases.[201]

These legislative proposals, however, ignore the political realities that make passage of this or similar legislation unlikely. The content and specificity of any legislation would "depend heavily on policy preferences," such that it could be drafted in either businesses' or consumers' favor.[202] Yet Congress's approach to data security has consistently suffered from bipartisan

193. *See* Isaacs, *supra* note 3, at 553–54.

194. Cave, *supra* note 176, at 789–93; Cease, *supra* note 174, at 420–21; Isaacs, *supra* note 3, at 554–57.

195. *See* Cave, *supra* note 176, at 790–91; Isaacs, *supra* note 3, at 557.

196. *See* Cave, *supra* note 176, at 793; Isaacs, *supra* note 3, at 556.

197. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (noting that future injury required that data thief "(1) read, copied, and understood [plaintiffs'] 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 [plaintiffs] by making unauthorized transactions in [their] names").

198. *See* Isaacs, *supra* note 3, at 555.

199. *Id.* at 556. Isaacs proposes consideration of several factors in determining reasonableness, including the type of data compromised, the amount the plaintiff stands to lose, and a plaintiff's actions with respect to a defendant's offer, if any, to pay for the credit monitoring. *Id.*

200. *See id.* at 554.

201. *See* Cave, *supra* note 176, at 787–89; *see also* discussion *supra* Sections II.B (standing) & III.B (damages).

202. Cease, *supra* note 174, at 421.

disagreement that has defeated, for instance, numerous bills that would have imposed stricter requirements on businesses to notify consumers following a data breach.[203] Moreover, even if a bill were to pass, states' different approaches and legislators' policy preferences would likely decrease its effectiveness.[204] These problems suggest that a legislative approach might not adequately address the current issues with increased risk standing.

Judicial adoption of the framework discussed above is therefore the preferable implementation method. Cave's objection to judicial resolution depends on the assumption that, to find standing and damages based on increased risk of identity theft, courts would have to substantively change the law.[205] But this belief is mistaken; permitting claims based on increased risk is consistent with traditional standing and damages principles.[206] Indeed, the tests that Isaacs outlines for inclusion in data-breach legislation strongly resemble those that this Note has articulated, which themselves arise from various courts' applications of standing and damages doctrines.[207] In addition, the concern over inconsistent standing and damages law is mitigated by a reframing of the circuit split as to increased risk standing[208] and the existing support for credit-monitoring damages by analogy to medical-monitoring claims.[209] These interpretations, although limited in their application thus far, provide an adequate foundation from which courts can shape their understanding of increased risk of identity theft as a basis for standing.

Moreover, leaving the ultimate resolution of increased risk standing to courts instead of legislatures better serves Article III's main purposes.[210] Because modifying the standing analysis to better account for claims based on increased risk of identity theft does not require a substantive change to the law,[211] the judiciary is just as capable as the legislature of properly effectuating this adjustment, negating any separation-of-powers concern. Furthermore, allowing courts to structure the proposed framework gives courts more flexibility in determining imminence on a case-by-case basis. The judicial-efficiency principle seeks to avoid an abundance of frivolous lawsuits.[212]

---

203. Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1195–96 (2014) (citing Christin McMeley, *Federal Data Breach Legislation Introduced, but Will It Go Anywhere?*, JD SUPRA BUS. ADVISOR (June 25, 2013), http://www.jdsupra.com/legalnews/federal-data-breach-legislation-introduc-74498 [http://perma.cc/34S4-W9N5]); *see also* Cave, *supra* note 176, at 780 & n.104 (citing "numerous" failed "comprehensive data privacy bills").

204. *See infra* notes 213–214 and accompanying text.

205. *See* Cave, *supra* note 176, at 785–87.

206. *See* discussion *supra* Sections II.B.3, III.B.

207. *Compare supra* notes 198–199 and accompanying text, *with supra* notes 188–191 and accompanying text.

208. *See* discussion *supra* Section II.B.3.

209. *See* discussion *supra* Section III.B.

210. *See supra* notes 36–37 and accompanying text.

211. *See* discussion *supra* Sections II.B.3, III.B.

212. *See* sources cited *supra* note 37.

Any statute regarding data-breach standing would have to be broadly drafted given the wide range of state approaches to data breaches[213] and the broad spectrum of legislators' policy preferences.[214] As a result, a legislative solution would not improve upon *Pisciotta*'s and *Krottner*'s improperly broad approach to increased risk of identity theft.[215] Giving courts the power to develop this framework would allow them to more effectively reject claims based on future injury that is not imminent enough to create Article III standing.

Conclusion

Given the increasing rate of data breaches and the failure of companies to appropriately respond, consumers will continue to suffer increased risks of identity theft when their personal information is exposed. Because current consumer-protection statutes do not provide adequate response mechanisms for data breaches, consumers must use the judicial system to hold companies responsible for their role in causing those injuries. Although *Pisciotta* and *Krottner* reached the right result in recognizing standing based on increased risk, their approach must be narrowed to allow only those claims that are most likely—because of their underlying facts—to satisfy both standing and damages inquiries. Applying this narrowed standing framework through courts alone will avoid the overexpansion of increased risk claims and respect the dual purposes on which the standing doctrine rests.

213. *See* BakerHostetler, State Data Breach Law Summary (2015), http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf [http://perma.cc/PX2Y-RRLX].

214. *See supra* note 202 and accompanying text.

215. *See supra* notes 170–171 and accompanying text.