Vanderbilt Law Review

Volume 73
Issue 5 *Issue 5 - October 2020*

Article 5

10-2020

The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution

Devin Urness

The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution

Data breaches are not going away. Yet victims still face uncertainty when deciding whether and where to file cases against companies or other institutions that may have mishandled their information. This is especially true if the victims have not yet experienced a financial harm, like identity theft, as a result of a data breach. Much of the uncertainty revolves around the standing doctrine and the Supreme Court's guidance (or lack thereof) on what constitutes a substantial risk of harm sufficient to establish an injury in fact. Federal circuit courts have come to divergent results in data breach cases based on the Supreme Court's guidance. This Note analyzes these divergent results and shows that the circuits are not as far apart as some commentators have suggested.

This Note then proposes two possible clarifying measures—one judicial and one legislative. The judicial solution is a test the Supreme Court should adopt for evaluating standing in data breach litigation. The test would have courts assess three factors and would allow plaintiffs who have not yet had their data misused to establish standing. Under the test, courts would examine (1) whether the breach was targeted; (2) whether the thief attained information that could lead to financial harm; and (3) whether any portion *of the compromised data has been misused. For the legislative solution, this Note proposes language for a private right of action that could be inserted into federal legislation, either as part of comprehensive privacy legislation or in sector-specific privacy legislation.*

INTRODUCTION

A customer buys some food for the week at the grocery store and uses a credit card for the purchase.[1] Two months later, the grocery store informs her that a software intrusion has led to the unauthorized disclosure of her name, credit card number, expiration date, card verification value ("CVV"), and personal identification number ("PIN").[2] She is not alone, and she teams up with fifteen other plaintiffs to sue the company for negligence.[3] Does she have standing to sue if no one has yet misused her data? The answer partially depends on where she sues.

Certain United States Courts of Appeals have held that plaintiffs lack standing[4] if they cannot demonstrate a thief or hacker has misused the compromised data.[5] Others have disagreed, holding that a data breach can create a substantial risk of harm sufficient to confer standing.[6] This Note posits that the circuits' underlying reasoning is not as inconsistent as the results in the cases would

1. This scenario is borrowed from *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 766 (8th Cir. 2017). The facts have been slightly modified in this first sentence.

2. *Id.* at 766.

3. *Id.*

4. The Supreme Court has consistently held that under the "Cases" and "Controversies" limitation in Article III, plaintiffs must demonstrate that they have standing in order for federal courts to have jurisdiction to adjudicate the plaintiffs' claims. U.S. CONST. art. II, § 2; *see* Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 37–38 (1976) (noting the constitutional roots of standing). A plaintiff must demonstrate three things to show that they have standing: injury in fact, causation, and redressability. Camreta v. Greene, 563 U.S. 692, 701 (2011) ("The party invoking the Court's authority has [standing] when three conditions are satisfied: The petitioner must show that he has 'suffered an injury in fact' that is caused by 'the conduct complained of' and that 'will be redressed by a favorable decision.' " (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992))). This standing doctrine ensures that plaintiffs have a "personal stake" in the suit. Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009) (internal quotation marks omitted). More detail on the jurisprudential roots of standing is in Section I.A.

5. *See infra* notes 83–86 and accompanying text (collecting cases).

6. *See infra* notes 87–90 and accompanying text (collecting cases).

suggest. Rather, differences in the facts between the cases explain some of the varying results.

For instance, one circuit court held that a plaintiff lacked standing when the plaintiff could not demonstrate misuse after someone stole a laptop containing the plaintiff's medical information.[7] Conversely, another circuit held that plaintiffs did have standing after pleading that their credit card information was stolen when hackers breached the servers of an online shoe retailer.[8] These cases seemingly reside on opposite sides of a "split" based on their results, but the underlying reasoning of each court focuses on similar factors. These factors help courts assess whether the plaintiff has demonstrated a "substantial risk" of injury sufficient to create an injury in fact,[9] and the limited "splits" in the circuits are a result of the varied applications of those individual factors.[10]

In addition to a plaintiff's facts, which are important for the standing analysis, the type of claim also partially explains the divide in the circuits' results. If a claim is based on a private right of action in a statute, plaintiffs who may otherwise have insufficient evidence to create an injury in fact can rely on Congress's definition of what constitutes an injury. As these fault lines in the circuit results show, data breach litigation is complicated. But extracting the differences in facts and claims in the circuit precedent can help ensure that plaintiffs and litigants craft the best possible case to garner standing.

Data breaches are on the rise,[11] meaning class action data breach litigation is likely to remain a mainstay on federal court dockets. Both institutions and individuals face challenges in responding to these breaches. On one side, after experiencing a breach, companies and other breached entities have to comply with myriad state data breach laws that may sometimes contradict one another.[12] On the other side, even if

7. Beck v. McDonald, 848 F.3d 262, 266–67 (4th Cir. 2017).

8. *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1023 (9th Cir. 2018), *cert. denied sub nom.* Zappos.com, Inc. v. Stevens, 139 S. Ct. 1373 (2019) (mem.).

9. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 n.5 (2013) (describing factors that create a substantial risk of injury sufficient to create an injury in fact, such as plaintiffs having "to reasonably incur costs to mitigate or avoid [a] harm").

10. *See infra* Section II.A (explaining how various circuits have applied the factors).

11. *See* James Coker, *278% Rise in Leaked Government Records During Q1 of 2020*, INFOSECURITY (Apr. 15, 2020), https://www.infosecurity-magazine.com/news/rise-leaked-government-records/ [https://perma.cc/4836-NLZ7] (noting that in the first quarter of 2020, 278% more government records were released than in the first quarter of 2019); James Sanders, *Data Breaches Increased 54% in 2019 So Far*, TECHREPUBLIC (Aug. 15, 2019, 7:35 AM), https://www.techrepublic.com/article/data-breaches-increased-54-in-2019-so-far/ [https://perma.cc/QNL5-XNVZ] (reporting that 2019 has seen a greater than fifty percent increase in breaches compared to the previous four years).

12. *Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security: Hearing Before the Subcomm. on Consumer Prot. & Commerce of the*

individuals whose personal information has been compromised do not experience identity theft immediately, they face the prospect of increased risk of identity theft and spending time and money on credit monitoring or other preventative measures, as well as potential anxiety or emotional stress as they wait for potential misuse.[13] Though these realities may seem like they harm the lives of the data breach victims, courts have often found that they do not satisfy the "injury in fact" requirement of Article III standing because they are "too speculative."[14]

This Note breaks down the circuit split on standing in data breach cases and suggests the factual complexity of data breach cases is obscuring a test for post-breach standing—a test that is already developing in the circuits. Part I provides the relevant background on standing and private rights of action in federal consumer privacy statutes. Section II.A then examines the circuit court split over whether the mere fact of a data breach creates a "substantial risk" of injury. Section II.A particularly focuses on three factors that form a common thread through many of the cases involved in the split: the intentionality of the breach; the nature of the breached information; and the misuse of part, but not all, of a compromised data set. Section III.A proposes that the Supreme Court employ a test comprised of these three factors when determining whether data breach victims have standing. Such a test would provide clarity to the circuits and resolve the circuit divisions over whether a breach leads to a "substantial risk" of injury. Without more guidance from the Supreme Court on what constitutes a "substantial risk," however, the proposed test may still leave many data breach victims unable to demonstrate injury in fact sufficient for standing. In order to address those left behind by the test, this Note proposes a second, legislative solution: a federal private right of action.

H. Comm. on Energy & Commerce, 116th Cong. 1 (2019) (statement of Christine S. Wilson, Comm'r, Fed. Trade Comm'n) ("The passage of the California Consumer Privacy Act and the prospect of bills in at least a dozen states have created confusion and uncertainty in the business community. This confusion is particularly acute because provisions in various state bills may contradict each other.").

13. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 750–54 (2018) (laying out the increased-risk-of harm, costs associated with preventing harm, and anxiety as the three main injuries cited by those that have not experienced identity theft).

14. *Beck* is perhaps the leading example, but lower courts have also found the injury to be too speculative. Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017); *see, e.g.*, Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 532 (D. Md. 2016) (holding that plaintiffs need to put forth facts that provide either actual examples of attempted use of the personal information or "a clear indication" that the hackers wanted the information to use in identity fraud in order to properly allege an injury in fact arising from an increased risk of identity theft); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) (holding that a class did not have standing when it commenced the suit three weeks after a breach).

Section II.B analyzes the Supreme Court's standing jurisprudence as it applies to private rights of action in data privacy cases, and Section III.B proposes simple language for lawmakers wanting to ensure that data breach victims get their day in court. The legislative solution in Section III.B would create an injury in fact for all data breach plaintiffs, dispelling the need for the test in Section III.A. The Supreme Court has declined to address whether stolen data creates a substantial risk of injury,[15] leaving uncertainty among the circuits. To remedy that uncertainty, Section III.B suggests a cure-all, blanket solution that Congress could adopt in the face of judicial inaction.

I. BACKGROUND

The judicial and legislative branches each have roles to play in clarifying whether the risk of identity theft after a data breach is a sufficient risk to confer standing. This Part first addresses how the judicial branch has created uncertainty, laying out the relevant doctrinal groundwork of Article III standing and demonstrating that the Supreme Court has left the circuits with relatively little guidance on what constitutes an injury in fact.

In the last decade, the United States Supreme Court issued two landmark decisions relevant to the Article III standing analysis: *Clapper v. Amnesty International USA*[16] and *Spokeo, Inc. v. Robins* (*Spokeo I*).[17] In combination, these decisions have created confusion in the federal circuits, leading to a division over what type of harm is "concrete" and "imminent" enough to rise to the level of an injury in fact. In data breach litigation specifically, circuits have come to different results on whether data breach victims have standing even if they cannot demonstrate misuse of their compromised data.[18]

15. CareFirst, Inc. v. Attias, 138 S. Ct. 981, 981 (2018) (mem.) (denying certiorari on "[w]hether a plaintiff has Article III standing based on a substantial risk of harm that is not imminent and where the alleged future harm requires speculation about the choices of third-party actors not before the court." Petition for Writ of Certiorari at i, *CareFirst*, 138 S. Ct. 981 (No. 17-641) (2017)).

16. 568 U.S. 398 (2013).

17. 136 S. Ct. 1540 (2016).

18. *Compare Beck*, 848 F.3d at 266 (holding that the risk of future identity theft was "speculative" where plaintiffs did not plead that the thieves intended to steal the breached data), *and In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 768–70 (8th Cir. 2017) (holding that it was not concrete enough to plead that generally, forty percent of those whose credit card numbers are compromised experience fraud the following year), *with* Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding that standing existed and explaining that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"), *and* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs'

Subsection I.A traces the roots of the injury-in-fact confusion, focusing particularly on the implications for data breach litigants.

On the legislative side, as is the dominant trend in many areas of privacy law,[19] Congress has not passed a statute devoted to addressing all data breaches—much less one with a private right of action.[20] Some privacy advocates and legal scholars have suggested that a federal private right of action for data breach victims may resolve the standing split among the circuits.[21] Subsection I.B explains how legislatively created private rights of action function, specifically with regard to a number of privacy statutes. Those private rights of action provide narrow avenues of relief for certain plaintiffs that may not have otherwise been able to demonstrate an injury in fact.

A. The Development of Article III Standing and Data Breach Litigation

Article III standing ensures that federal courts pass judgment only on "[c]ases" and "[c]ontroversies"[22] and that "a specific person is the proper party to bring a matter to the court."[23] In the mid-twentieth century, that standard meant individuals with a private, but not public, right could seek recourse in the courts.[24] The doctrine developed into three elements that a plaintiff must prove in order to allow the court to hear her case: (1) an injury in fact that demonstrates an "invasion of a legally protected interest"; (2) a causal nexus between the injury and

complaints."); *see also* Brandon Ferrick, Comment, *No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions*, 59 B.C. L. REV. E. SUPP. 462 (2018) (explaining the circuit split and advocating for the Fourth Circuit's approach, which rejects the risk of identity theft as an injury-in-fact sufficient to confer standing).

19. *See* Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1464 (2017) (noting the federal government has lagged in responding to privacy problems).

20. *See* Justin H. Dion & Nicholas M. Smith, *Consumer Protection—Exploring Private Causes of Action for Victims of Data Breaches*, 41 W. NEW ENG. L. REV. 253, 267–72 (2019) (summarizing the federal data protection laws).

21. *See, e.g.*, *id.* (advocating for an amendment to the Federal Trade Commission Act to permit individuals to sue to enforce data breach response violations); Michael Hopkins, Comment, *Your Personal Information Was Stolen: That's an Injury: Article III Standing in the Context of Data Breaches*, 50 U. PAC. L. REV. 427 (2019) (proposing language for a private right of action based on California's data breach notification law as it stood in 2015).

22. U.S. CONST. art. III, § 2.

23. ERWIN CHEMERINSKY, FEDERAL JURISDICTION 55 (7th ed. 2016).

24. *See* Coleman v. Miller, 307 U.S. 433, 464 (1939) ("No matter how seriously infringement of the Constitution may be called into question, this is not the tribunal for its challenge except by those who have some specialized interest of their own to vindicate, apart from a political concern which belongs to all.").

the defendant's conduct; and (3) redressability of the injury.[25] Since the late twentieth century, the Court has required a more established injury in fact, mandating a plaintiff show an injury that is "concrete, particularized, and actual or imminent."[26]

At the same time, the Supreme Court has emphasized that standing is not a particularly onerous requirement: plaintiffs can satisfy standing with "general factual allegations of injury resulting from the defendant's conduct."[27] But while the requirement may not be designed to be onerous, the Court's decisions in *Clapper* and *Spokeo* combine to create a morass for circuits trying to determine whether plaintiffs have standing in data breach litigation.

In *Clapper*, the Court held that future injuries suffice to create standing as long as they are "certainly impending." At the same time, the Court also noted that a "substantial risk" of harm has been sufficient to satisfy the injury in fact element of standing in the past.[28] In the case, public interest groups and various individuals brought suit against the U.S. government, challenging a national security law—the FISA Amendments Act of 2008—and alleging that the law would allow the government to surveil communications with individuals outside the United States.[29] The plaintiffs argued they had standing because the government was likely to surveil their communications and because they had to take precautions to keep the government from intercepting the communications.[30] After noting that an "especially rigorous" review of standing was required because of the national security and separation of powers implications of the case,[31] the Court laid out the two tests for determining whether future injuries qualify as injuries in fact: the "certainly impending" test and the "substantial risk" test.[32]

Applying the stricter and more rigorous "certainly impending" test—possibly because of the national security implications—the Court

25. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

26. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).

27. *Lujan*, 504 U.S. at 561; *see also* Gladstone, Realtors v. Vill. of Bellwood, 441 U.S. 91, 99 (1979) ("In order to satisfy [U.S. Const.] Art. III, the plaintiff must show that he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant.").

28. *Clapper*, 568 U.S. at 409, 414 n.5.

29. *Id.* at 406.

30. *Id.* at 407.

31. *Id.* at 408–09.

32. *See id.* at 409, 414 n.5:

> Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.

held that the likelihood of the government surveilling plaintiffs' communications was based on "mere conjecture about possible governmental actions."[33] The Court stood by its "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors."[34] Next, the Court held that for standing purposes, costs accrued in response to a future harm constitute an injury only if the underlying future harm is "certainly impending" or imminent.[35] Despite the outcome in *Clapper*, the "substantial risk" test did not go away: a year after the *Clapper* decision, the Court repeated that a future injury is an injury in fact if there is "a 'substantial risk' that the harm will occur."[36] Given the lack of separation of powers or national securities issues involved in data breach cases, the "substantial risk" test has become the standard that circuits—on both sides of the divergent results—use for data breach litigants.[37]

The Court's decision in *Spokeo*, issued two years after *Clapper*, sheds light on another possible avenue to establish a sufficiently concrete injury in fact: a congressionally created interest. In *Spokeo*, the plaintiff sued Spokeo under a private right of action provided in the Fair Credit Reporting Act ("FCRA") for "willfully fail[ing]" to "follow reasonable procedures" in maintaining the accuracy of information that would affect his creditworthiness.[38] The Court held that—without more—a "bare procedural violation" like distributing an incorrect zip code for an individual is not sufficiently concrete to confer standing based on an injury under the FCRA.[39] The Court remanded the case to the Ninth Circuit, requiring a more in-depth concreteness analysis.[40]

33. *Id.* at 420.

34. *Id.* at 414.

35. *See id.* at 416:

> Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. . . . [R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.

36. *See* Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting *Clapper*, 568 U.S. at 414 n.5) (addressing whether the threat of future law enforcement could confer standing). The *Driehaus* Court did not elaborate on the substantial risk test beyond asserting that it was a possible avenue for establishing injury in fact. *Id.*; *see also* Nicholas Green, *Standing in the Future: The Case for a Substantial Risk Theory of "Injury in Fact" in Consumer Data Breach Class Actions*, 58 B.C. L. REV. 287, 304–05 (2017) (arguing that a Supreme Court majority would likely support a "substantial risk" test in data breach litigation).

37. *See, e.g.*, *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1024, 1029 (9th Cir. 2018) (finding standing based on a "substantial risk" of future harm after a breach); Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (denying standing based on a lack of "substantial risk").

38. *Spokeo I*, 136 S. Ct. 1540, 1545 (2016).

39. *Id.* at 1550.

40. *Id.*

On remand, the Ninth Circuit held that the FCRA does establish a sufficiently concrete interest, offering hope to litigants trying to establish standing based on intangible harms.[41]

While some consumer protection statutes, like the FCRA, allow data breach litigants to establish standing through a congressionally created private right of action,[42] the patchwork of federal consumer protection statutes leaves many data breach litigants to rely on possible future identity theft to establish standing.[43] As a result, evaluating standing in data breach litigation has turned into a highly fact-sensitive inquiry that closely mirrors the substantive evaluation of the underlying claims, especially when examining the injury-in-fact requirement.[44]

Plaintiffs who have not yet experienced identity theft resulting from a breach typically argue one of three injuries: risk of identity theft (a future injury), time and money spent on credit monitoring or other preventative measures (a present injury), or anxiety or emotional stress (a present injury).[45] In the absence of a private right of action and a statutorily created interest, plaintiffs have to argue that identity theft is a concrete injury and that the risk is sufficiently imminent to make it a "substantial risk" under *Clapper*.[46] When assessing the imminence of a future identity theft based on the Supreme Court's limited guidance in *Clapper*, courts have implicitly looked at the following factors to determine whether the threat rises to the level of a substantial risk: (1) the presence of intent to specifically take the breached data,[47] (2) the

41. Robins v. Spokeo, Inc. (*Spokeo II*), 867 F.3d 1108, 1112–13 (9th Cir. 2017).

42. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 640–41 (3d Cir. 2017) (finding standing based on a statutory interest underlying the FCRA).

43. *See infra* Section II.B (discussing federal consumer protection statutes with a private right of action).

44. *See* Solove & Citron, *supra* note 13, at 748 (arguing that the harm analysis is often determinative for data breach cases and often leads to early dismissal).

45. *See id.* at 750–54 (laying out the increased-risk-of harm, costs associated with preventing harm, and anxiety as the three main injuries cited by those that have not experienced identity theft).

46. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409, 414 n.5 (2013); *see, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017):

> "[T]he proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case would be identity theft, "as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes." . . . Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury.

(quoting Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 915 (D.C. Cir. 2015)).

47. *See Attias*, 865 F.3d at 628–29 (applying the substantial risk test and holding that it is not speculative to infer that a hacker has the "intent and the ability" to use the accessed personal information); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a . . . database and steal consumers' private information? Presumably,

type of data released,[48] and (3) the misuse of *any* of the data accessed during a breach.[49]

Unfortunately, the courts have relied on these factors without stating as much, leading numerous plaintiffs to inadequately plead injury.[50] Furthermore, application of these factors—particularly the first factor—leaves courts attempting to assess the intent of a nonparty.[51] Perhaps predictably, assessing intent has also contributed to the divergent results: some circuits view the theft of consumer data as sufficient to create an inference of intentionality, while others look for more.[52] These divergent results present confusion post-*Clapper* and post-*Spokeo*. Part II will further analyze the divergent results and highlight the splits within the factors. Notably, unlike the plaintiff in *Spokeo*, the plaintiffs mired in the divergent results are only stuck because they are unable to establish another concrete interest besides the threat of future injury; they cannot point to a statutory interest that has been violated and can be vindicated through a private right of action.[53]

the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.").

48. *Compare* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) ("And [plaintiff] does not allege how she can plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information—such as her birth date or Social Security number—is alleged to have been stolen."), *with* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385–86 (6th Cir. 2016) (conferring standing when a breached databased contained personal information such as "names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers").

49. *See, e.g.*, *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 56 (D.C. Cir. 2019) (finding that there was a substantial risk of harm from future identity theft because part of the class had already "experienced various types of identity theft, including the unauthorized opening of new credit card and other financial accounts and the filing of fraudulent tax returns in their names").

50. *See, e.g.*, *Whalen*, 689 F. App'x at 90–91 (holding that the plaintiff failed to plead that she spent any time or money monitoring her credit even when she pled that the thief had tried to use her card after she changed the number).

51. Assessing the intent of a third party was a large issue in *Clapper*, and assessing the intent of the thief is the main problem with the analysis for courts that hold that a breach alone is enough to confer standing. *See* 568 U.S. at 413–14.

52. *Compare In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 767, 774 (8th Cir. 2017) (holding that plaintiffs did not have standing after alleging that their credit card information was stolen in a software intrusion because there was no evidence that the stolen information had been used), *with Attias*, 865 F.3d at 630 (conferring standing after the hack of a health-care company).

53. *See Spokeo II*, 867 F.3d 1108, 1112–13 (9th Cir. 2017) (discussing the need for plaintiffs to show a "real" injury and relying on congressional judgment as to what qualifies as a "real" intangible injury when deciding whether to confer standing).

B. Private Rights of Action and Standing

Scholars and advocates have suggested a number of solutions to resolving the circuit split over whether to confer standing based on increased risk of identity theft. Some scholars have advocated for reconceptualizing how courts think about probabilistic injuries, including acknowledging risk and anxiety as harms in data breach cases, as courts have done in other contexts.[54] Other commentators have argued for the Supreme Court to recognize a right to privacy for personal data.[55] Beyond ameliorating the Article III standing issues, inserting into federal legislation a private right of action that recognizes an individual's right to sue for actual damages ensuing from a breach—an approach many states have taken—is popular among privacy advocates.[56] But, for standing in particular, legal commentators have suggested a private right of action may create an imminent and concrete interest that confers standing.[57]

The most recent guidance from the Court on when injuries are sufficiently "concrete" came in *Spokeo*, which concerned an alleged violation of the FCRA.[58] The FCRA contains a private right of action: "[A]ny person who willfully fails to comply with any requirement [of the Act] with respect to any consumer is liable to that consumer" for "actual damages" or statutory damages, as well as attorney's costs and fees.[59] The plaintiff asserted his private right to sue by arguing that Spokeo, as a consumer reporting agency, had willfully failed to follow certain statutory requirements.[60] When reviewing the Ninth Circuit's standing

54. *See* Solove & Citron, *supra* note 13, at 756–73 (pointing to increased recognition of injuries based on future probabilistic injuries, including risk of future injury in medical malpractice cases, and to growing acceptance of anxiety and emotional distress as a harm); *see also* Jonathan Remy Nash, *Standing's Expected Value*, 111 MICH. L. REV. 1283 (2013) (proposing the use of expected value in assessing injury in fact).

55. *See* Nick Beatty, Note, *Standing Room Only: Solving the Injury-in-Fact Problem for Data Breach Plaintiffs*, 2016 BYU L. REV. 1289, 1290–91 (2016) (analyzing *Clapper* and *Spokeo* and suggesting that recognizing a right to privacy would suffice to create a concrete injury).

56. *See, e.g.*, Ams. for Fin. Reform et al., *The Time Is Now: A Framework for Comprehensive Privacy Protection and Digital Rights in the United States*, CONSUMER FED'N AM. 2 (Apr. 19, 2019), https://consumerfed.org/wp-content/uploads/2019/01/4.19Privacy-and-Digital-Rights-For-All-Framework.pdf [https://perma.cc/J93T-X7ZQ] (advocating for a private right of action as an integral part of enforcing privacy rights).

57. *See, e.g.*, 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, 769 (2013) (arguing for a private right of action in federal legislation); Elizabeth T. Isaacs, Comment, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 554–56 (2015) (suggesting that a private right of action would remove standing as a barrier to recovery for data breach victims).

58. *Spokeo I*, 136 S. Ct. 1540, 1549 (2016).

59. 15 U.S.C. § 1681n(a) (2012).

60. *Spokeo I*, 136 S. Ct. at 1545.

analysis, the Supreme Court held the Ninth Circuit's analysis was incomplete because it did not properly assess whether the plaintiff's injury was concrete—that is, whether it "actually exist[ed]."[61] Remanding the case to the Ninth Circuit, the Court made clear that certain intangible injuries may be concrete.[62] Importantly, the violation of a statute with a private right of action is an intangible injury that can confer Article III standing as long as it is not a "bare procedural violation."[63] The Court identified two factors that contribute to whether a statutory violation is not "a bare procedural violation" and rises to the level of a "concrete" injury: (1) "[W]hether 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," and (2) Congress's "judgment . . . . Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.' "[64]

On remand, the Ninth Circuit applied the Court's new concreteness analysis.[65] The court held that the concrete injury Congress intended to protect through the relevant provision of the FCRA was the transmission of inaccurate information that would affect an individual's credit report and that the plaintiff could sue to enforce that provision. The Ninth Circuit created a new standing test for plaintiffs seeking to vindicate purported statutory rights: Were the statutory provisions at issue "established to protect . . . concrete interests (as opposed to purely procedural rights)[?]" And if so, do "the specific procedural violations alleged in this case actually harm, or present a material risk of harm to, such interests[?]"[66] The formulations of the Supreme Court's and the Ninth Circuit's tests would prove instructive for litigants seeking to establish a concrete statutory interest sufficient to confer standing.[67]

The Ninth Circuit's new test relies on the language of a specific statute, and a number of federal statutes implicating privacy rights already contain private rights of action. The Fair and Accurate Credit

61. *Id.* at 1548.

62. *Id.* at 1549.

63. *Id.*

64. *Id.* (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)). In data breach litigation and data privacy litigation more generally, both of these factors play a role in assessing whether a statute has created a sufficiently concrete injury to rise to the level of "legally cognizable." *See infra* Section III.B (discussing how some courts have found standing based on statutory interests' similarities to common law torts).

65. *Spokeo II*, 867 F.3d 1108, 1112–13 (9th Cir. 2017).

66. *Id.* at 1113.

67. *See infra* Section III.B (discussing how plaintiffs have tried to use private rights of action to establish standing).

Transactions Act ("FACTA") amended the FCRA in 2003 to better protect individuals from identity theft and to allow individuals to sue to enforce certain provisions.[68] Like the FCRA, the Cable Communications Policy Act ("CCPA"), which requires cable operators to "destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected," also allows individuals to sue for enforcement.[69] However, despite numerous efforts at the federal level,[70] Congress has failed to enact a statute that covers all data breaches, not just those concerning consumer reporting agencies or cable operators. Furthermore, following *Spokeo*, some federal courts have limited the reach of private rights of action, thus limiting litigants' ability to demonstrate standing.[71] More importantly for data breach litigants, many consumer protection statutes featuring private rights of action do not apply to the breached entities, preventing the victims from asserting the statutory interest.

In the absence of broad federal action, states have led the charge on data privacy legislation, and a number of states have included private rights of action in statutes specifically devoted to giving individuals legal recourse when their data is released.[72] Breach notification statutes require breached entities to notify those who have had their personal information accessed.[73] These notification statutes were central in setting rules of the road for how companies or government agencies should respond to a breach.[74] Today, all fifty

68. *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (amending the FCRA); *In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 630, 641 (3d Cir. 2017) (holding that plaintiffs had standing when they sued under the FCRA's private right of action and argued that the defendant had improperly "furnished" information in violation of the FCRA).

69. Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 910 (7th Cir. 2017).

70. *E.g.*, Personal Data Notification and Protection Act of 2017, H.R. 3806, 115th Cong. (2017) (seeking to establish a national standard with regard to data breach notification); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014) (detailing that the purpose of the bill is to "prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information").

71. *See infra* Section III.B (discussing private rights of action and their application to data breach suits).

72. *See* Taryn Elliott, Comment, *Standing a Chance: Does* Spokeo *Preclude Claims Alleging the Violation of Certain State Data Breach Laws*, 49 SETON HALL L. REV. 233, 242–47 (2018) (detailing the development of private rights of action, specifically in California, Washington, and New Hampshire).

73. *See* Michael Bloom, Note, *Protecting Personal Data: A Model Data Security and Breach Notification Statute*, 92 ST. JOHN'S L. REV. 977, 987–88 (2018) (generally describing covered entities and notification requirements).

74. California was the first to pass such a law, and did so in 2003. *See* Press Release, Office of the Att'y Gen. of Cal., Attorney General Becerra and Assemblymember Levine Unveil Legislation to Strengthen Data Breach Notification Law (Feb. 21, 2019), https://oag.ca.gov/news/press-releases/attorney-general-becerra-and-assemblymember-levine-unveil-legislation-

states have some form of a breach notification statute.[75] Many of these statutes give a certain number of days by which notification must occur and also require that notification occurs without "unreasonable delay."[76]

Current enforcement of these notification statutes is largely based on attorneys general and civil penalties, not private rights of action.[77] Civil penalties are a standard punishment, and a state may allow its attorney general to enforce violations on behalf of victims[78] or rely on the attorney general to enforce on behalf of the state.[79] Penalties from delayed notification may create incentives to tell consumers in a reasonable time.[80] But absent additional evidence of misuse to sustain a more traditional negligence claim, consumers are still generally left without recourse when they are not notified within a reasonable time that their information has been compromised.[81]

strengthen [https://perma.cc/ZTZ4-VEPT] ("In 2003, California became the first state to pass a data breach notification law requiring companies to disclose breaches of personal information to California consumers whose personal information was, or was reasonably believed to have been, acquired by an unauthorized person.").

75. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/ERX7-M2AW] (compiling statutes).

76. *See, e.g.*, ALA. CODE § 8-38-5(b) (2018) ("[W]ithout unreasonable delay" with a 45-day maximum); FLA. STAT. § 501.171(3)(a) (2019) ("[A]s expeditiously as practicable" with a 30-day maximum); *see also* Substitute H.B. 1071, 66th Leg., Reg. Sess. § 2 (Wash. 2019) (amending WASH. REV. CODE § 19.255 (2019) to shorten the maximum allotted time for covered entities to respond from forty-five to thirty days).

77. *See* Madelyn Tarr, *Law Firm Cybersecurity: The State of Preventative and Remedial Regulation Governing Data Breaches in the Legal Profession*, 15 DUKE L. & TECH. REV. 234, 239 (2017) (outlining the general differences in timing and enforcement in state notification statutes).

78. *E.g.*, N.Y. GEN. BUS. LAW § 899-aa (LexisNexis 2019).

79. *See, e.g.*, ARIZ. REV. STAT. ANN. § 18-552(L) (2019) ("[O]nly the attorney general may enforce . . . a violation . . . ."); IDAHO CODE § 28-51-107 (2019) ("[T]he primary regulator may bring a civil action to enforce compliance . . . .").

80. *See* People v. Uber Techs., No. CGC-18-570124, 2018 Cal. Super. LEXIS 5119, at *5–15 (Sept. 26, 2018) (detailing the steps that Uber must take after delaying breach notification and committing other statutory violations, including paying $148 million in penalties that were split among various states and complying with a Breach Notification Plan overseen by the California Attorney General); *see also* Press Release, Office of the Att'y Gen. of Cal., California Attorney General Becerra, San Francisco District Attorney Gascón Announce $148 Million Settlement with Uber over 2016 Data Breach and Cover-Up (Sept. 26, 2018), https://oag.ca.gov/news/press-releases/california-attorney-general-becerra-san-francisco-district-attorney-gasc%C3%B3n [https://perma.cc/88KY-VV9R] (summarizing the nationwide settlement).

81. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695 (7th Cir. 2015) (noting that "delay in notification is not a cognizable injury" meriting Article III standing (citing Price v. Starbucks Corp., 122 Cal. Rptr. 3d 174 (Ct. App. 2011))); Antman v. Uber Techs., Inc., No. 3:15-cv-01175-LB, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("Mr. Antman also did not plead injury related to the delay; delay alone is not enough."); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1217–18 (N.D. Cal. 2014) (concluding that the plaintiffs had not established Article III standing for their delayed notification claim because they had "not allege[d] that they suffered any incremental harm as a result of the delay").

II. ANALYSIS

A. The Three Factors That Contribute to Divergent Results in the Circuits

Divergent results in the circuits over whether the risk of future identity theft is sufficient to confer standing is not new; it has been developing since 2011.[82] As it stands, the Second,[83] Third,[84] Fourth,[85] and Eighth[86] Circuits have declined to extend standing based on a substantial risk of injury after an alleged breach. On the other hand, the D.C.,[87] Sixth,[88] Seventh,[89] and Ninth[90] Circuits have found that the

82. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 43–46 (3d Cir. 2011) (holding that alleged victims of data breach did not have standing and splitting from the Ninth Circuit, which decided *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), a year earlier).

83. *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90–91 (2d Cir. 2017) (holding that plaintiff lacked standing because she did not plead how her old credit card number could be linked to future identity theft after her credit card information was accessed during a breach and fraudulent charges were made on the card, but she never had to pay for the charges).

84. *See Reilly*, 664 F.3d at 45 (holding that the plaintiff lacked standing for lack of evidence that the hacker read, copied and understood the data). *But see In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639–41 (3d Cir. 2017) (holding that victims of breach had standing because FCRA claim was meant to protect against the same injury as common law actions and that Congress had thus intended to have FCRA violation count as legally cognizable injury).

85. *See* Beck v. McDonald, 848 F.3d 262, 271–76 (4th Cir. 2017) (holding that plaintiff did not have standing when there was no evidence that the thief stole laptop with intent to access the information).

86. *See In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 768–72 (8th Cir. 2017) (holding that risk of future identity theft was insufficient to confer standing when evidence was presented that victims of data breaches may not suffer identity theft for years or at all). *But see* Kuhns v. Scottrade, 868 F.3d 711, 715–16 (8th Cir. 2017) (finding plaintiff has standing based on losing the value of his bargain when defendant was contractually obligated to take reasonable safeguards to protect plaintiff's personal information but was still hacked).

87. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 54–61 (D.C. Cir. 2019) (conferring standing where there was evidence the Chinese conducted the hack and evidence of fraudulent charges for part of the class); Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (holding that standing exists "simply by virtue of the hack and the nature of the data" that was taken).

88. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 387–88 (6th Cir. 2016) (holding that plaintiff has standing based on statistics that data-breach victims are 9.6 times more likely to experience fraud and on the hours spent on fraud mitigation as a result of the breach).

89. *See* Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 828–30 (7th Cir. 2018) (finding that spending time notifying businesses of new account numbers and changing credit card numbers on accounts with automatic payments is sufficiently specific to qualify as an injury in fact); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding that the risk of future identity theft was substantial because the hack was "targeted" and was an intentional theft of credit card numbers); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634–40 (7th Cir. 2007) (equating risk of identity theft with the risk of exposure to toxic substances and the use of defective medical devices and finding that the risk was substantial enough to confer standing).

90. *See In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1027–29 (9th Cir. 2018) (finding that risk of identity theft after hack of credit card records was sufficient to confer standing and that the fact that part of class had experienced fraud raised the risk for the other part of the class); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010)

post-breach risk of injury is a substantial risk sufficient to establish standing. As with all cases, the first differentiator in many of these cases is the facts involved. Factual differences contribute to some, but not all, of the differing results in the circuits. The divergent results also center around the application of three factors: (1) whether the hack of an entity involved sufficient targeting of the stolen information to raise the threat of misuse to a substantial risk,[91] (2) the nature of the breached information,[92] and (3) whether any other victims of the breach have actually had their data misused.[93] The actual "splits" among the circuits are much smaller than the divergent results suggest.

The circuits are also divided over whether mitigation costs—which are present, not future, injuries—can confer standing, but following *Clapper*'s commands,[94] this divide is wholly dependent upon whether a court finds the underlying risk of misuse sufficiently substantial.[95] The Second Circuit is the only circuit to hold that a plaintiff lacked standing after she spent time and money in the aftermath of actual *attempted misuse* of her compromised data.[96] That decision was a bit of an outlier. Unlike many other data breach suits, which often become class actions, the plaintiff in that suit was the only plaintiff, making it more difficult for her to allege future misuse after she had already changed her credit card information.[97] The Second Circuit case is even more of an outlier because other circuits have held that evidence of attempted misuse amounts to an injury in fact,[98] and the plaintiff's attorneys failed to allege any specifics about the time or effort "that [the plaintiff] herself" expended monitoring her credit.[99]

(conferring standing based on the threat of future identity theft after company laptop containing unencrypted personal information was stolen).

91. *See infra* Section II.A (discussing the impact of intentionality on standing).

92. *See infra* Section II.A.2 (examining how the nature of the information breached affects standing).

93. *See infra* Section II.A.3 (illustrating the effect of proven misuses of breached data on the standing inquiry).

94. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013) ("[Plaintiffs] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

95. *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017) (refusing to grant standing because the plaintiff's claims of lost time and effort monitoring credit and finances were not specific enough).

96. *Id.* at 90–91.

97. *Id.* at 90.

98. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015) (holding that fraudulent charges that led to no money lost can lead to standing based on the loss of value of time and money spent in response).

99. *Whalen*, 689 F. App'x at 91. Listing the Second Circuit with the other circuits that have denied standing glosses over the facts of these individual cases, and once those facts are taken into account, a common thread appears focusing on the factors listed *infra*.

The more prototypical data breach suit leading to standing questions involves victims who spend time and money to prevent their information from being misused and file suit before any attempted misuse takes place.[100] The underlying harm then becomes future misuse—either potential identity theft or account fraud. In such cases, courts tend to base their decision to confer standing on a combination of the three factors above (intentionality, the nature of the data, and misuse of a segment of the breached data). Courts may deny standing because (1) there is insufficient intent to misuse the compromised data;[101] (2) the compromised data is not the type that could plausibly[102] lead to identity theft;[103] or (3) one plaintiff's demonstrated misuse does not increase the risk of identity theft for the other plaintiff-victims.[104] It is the combination of these factors—in addition to the varying facts—that makes analyzing the divergent results complex. This Part extracts the factors from the cases to show how the factors explain the divergent results in the circuits, and Section III.A proposes how the Supreme Court should deal with in any divisions within the factors.

1. Intentionality

Data breaches occur largely in one of two ways: an entity's informational security system is accessed by an unauthorized party, potentially leading to information being copied,[105] or a customer's information is physically stolen, often through the theft of a laptop

100. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (discussing incurrence of mitigation costs after social security numbers, customer names, and other personal information was stolen from a health insurer).

101. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) ("[P]laintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information.").

102. Because standing is a threshold issue, it is typically addressed through motions to dismiss at the pleading stage, meaning that plaintiffs must merely plausibly allege a substantial risk of harm. *See Attias*, 865 F.3d at 627 ("[K]eeping in mind the light burden of proof the plaintiffs bear at the pleading stage, [the question] is whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of [the defendant's] alleged negligence in the data breach."). Indeed, all the cases involved in the divergent results in the circuits were at the pleading stage. *See supra* notes 82–90 (collecting cases).

103. *Whalen*, 689 F. App'x at 90–91 (holding that there was no risk of future identity theft where the plaintiff had already changed her card information after it was compromised).

104. *See In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 769–74 (8th Cir. 2017) (denying standing to all plaintiffs, except the one that could demonstrate misuse).

105. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 42–46 (3d Cir. 2011) (holding that mere access without evidence of reading, copying, and understanding is insufficient to create a substantial risk of identity theft), *with* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 692–93 (7th Cir. 2015) (holding that identity theft was a substantial risk after a hack stealing credit card numbers).

containing such information.[106] Some circuits have been willing to find that plaintiffs claiming negligence have standing in both instances.[107] Others have denied that mere access by an unauthorized person creates a sufficient risk of identity theft[108] or that the theft of physical property plausibly implies that the contents of the property will be accessed and then used to harm the plaintiffs.[109] Those courts denying standing focus on the assumptions necessary to conclude that the plaintiffs will one day be subject to identity theft.[110] Of paramount concern to these courts is the assumption that the hacker, or a party to whom she sells the data, intends to use the compromised data for identity theft.

Beck v. McDonald from the Fourth Circuit serves as an illustrative example of an alleged breach from the theft of physical property. In that case, a Veterans Affairs ("VA") laptop was stolen from a hospital, and pathology records of patients were lost.[111] The class of plaintiffs sued, citing previously decided Sixth, Seventh, and Ninth Circuit decisions to argue that the unauthorized dissemination of their information by the VA put them at a substantial risk of identity theft.[112] The Fourth Circuit distinguished those cases by asserting that the data thief in those cases had "intentionally targeted" the compromised data; whereas, in this case, there was no evidence the person who stole the

106. *See, e.g.*, *Beck*, 848 F.3d at 266–67 (stolen laptop at veterans affairs hospital and lost pathology reports at same hospital); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (Starbucks laptop with unencrypted employee information); *In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 629–30 (3d Cir. 2017) (two of health insurer's laptops containing personal information).

107. *See Attias*, 865 F.3d at 628–29 (holding that plaintiffs had standing after breach of health insurer); *Krottner*, 628 F.3d at 1143 (finding standing after theft of laptop). Notably, this Section focuses on negligence claims rather than breach of contract claims because those claims are present, not future, injuries, and when plaintiffs plausibly plead a breach, courts confer standing. *See* Kuhns v. Scottrade, Inc., 868 F.3d 711, 715–16 (8th Cir. 2017) (holding that a plaintiff had standing when he could demonstrate that a company had agreed to protect his information and failed to do so); Katz v. Pershing, LLC, 672 F.3d 64, 72–75 (1st Cir. 2012) (holding that plaintiff did not have standing based on breach of contract because pleadings were insufficient to create even an implied contract).

108. *See In re SuperValu, Inc.*, 870 F.3d at 768–70 (finding lack of standing based on bare assertion that data breaches facilitate identity theft when no personally identifying information was stolen); *Reilly*, 664 F.3d at 43 (holding that allegations of an increased risk of identity theft resulting from a security breach are insufficient to secure standing).

109. *See Beck*, 848 F.3d at 273–76 (holding that laptop and records theft did not create a substantial risk of identity theft).

110. *See id.* at 269, 275 (listing the assumptions necessary to ultimately arrive at identity theft and holding that they were too speculative).

111. *Id.* at 266–67.

112. *Id.* at 274 (first citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); then citing Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007); and then citing *Krottner*, 628 F.3d at 1139).

laptop or who currently had the pathology reports did so with the intent or capability of using that information against the plaintiffs.[113]

In contrast, the Ninth Circuit faced similar facts in *Krottner v. Starbucks Corp.*, but came to the opposite result.[114] In that case, a laptop with personnel data of Starbucks employees was stolen, and the court held that the plaintiffs had pled an injury in fact because the prospect of future misuse by the thief presented an "actual injury" under a pre-*Clapper* injury-in-fact test.[115] *Krottner* and *Beck* present a true split over standing in physical breaches. But because *Krottner* was the first major data breach case decided pre-*Clapper*, the Fourth Circuit's analysis in *Beck* is more consistent with Supreme Court precedent. The Fourth Circuit's analysis also implicitly applies the intentionality test developed in the circuits by assessing whether the thief had targeted or stolen the laptop in order to steal the data contained on the laptop.[116] The Ninth Circuit, however, continues to cite *Krottner* as justification for finding an injury in fact in hacking cases, despite the Fourth Circuit's post-*Clapper* analysis.[117]

The second type of breach—hacked data—is more (in)famous because of the large numbers of records associated with the breaches.[118] Before describing the split over whether a hacker demonstrates sufficient intentionality to lead to a substantial risk of harm, it is helpful to address the First Circuit's decision in *Katz v. Pershing, LLC*.[119] In *Katz*, the plaintiff alleged that a company's security was insufficient and would allow for unauthorized access to the plaintiff's data.[120] The First Circuit denied standing because no unauthorized access had occurred yet, and the potential for breach was insufficient to create an injury.[121] The fact that no breach had occurred differentiates this case from the other cases in which courts conferred standing.[122]

113. *Id.*

114. 628 F.3d at 1140.

115. *Id.* at 1140, 1142.

116. *See Beck*, 848 F.3d at 274 (noting that plaintiffs made no claims that the laptop was targeted in order to steal the data it contained).

117. *See In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1023 (9th Cir. 2018) (holding that plaintiffs have sufficiently alleged standing based on the risk of identity theft).

118. *See* Tara Siegel Bernard, *Equifax Breach Affected 147 Million, but Most Sit Out Settlement*, N.Y. TIMES (Jan. 22, 2020), https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html [https://perma.cc/J3BP-D3HG] (noting that 147 million customers of Equifax were affected by the data breach that resulted in a massive settlement).

119. 672 F.3d 64 (1st Cir. 2012).

120. *Id.* at 78–80.

121. *Id.*

122. *Id.* at 80.

However, even if plaintiffs allege a breach, they can run into trouble if they cannot or do not plead that a thief downloaded or processed the plaintiffs' data, rather than alleging the thief merely gained access to it. [123] This precise scenario was at issue in *Reilly v. Ceridian*. The *Reilly* plaintiffs alleged that a hacker had penetrated a company's firewall, and the Third Circuit denied standing because the plaintiffs did not allege that the hacker "read, copied, and understood" the information.[124] Though both were decided pre-*Clapper*, *Reilly* and *Katz* help lay out how to analyze cases in which plaintiffs allege that their data has been negligently handled. Plaintiffs must allege a breach and allege that the breach led to a theft of their data.

Reilly also helped develop the intentionality factor. The Third Circuit differentiated *Reilly* from another breach case by arguing that a hacker merely accessing the information does not demonstrate the "intrusion was intentional."[125] Because the case was pre-*Clapper*, the Third Circuit applied the stricter "certainly impending" standard rather than the "substantial risk" test.[126] However, despite applying an old standard, *Reilly* is still important because of the Third Circuit's focus on the intentionality of the breach in the standing analysis.

Since *Reilly*, multiple circuits have assessed the intents of the hackers as a way of determining whether there is a "substantial risk" of data misuse.[127] The most often cited reasoning for finding adequate intent for standing comes from the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[128] In *Remijas*, a hacker stole the credit card numbers of Nieman Marcus customers.[129] In addition to its oft-cited rhetorical question, the circuit court reasoned there was a "substantial risk" under *Clapper* because there was no need to speculate that the customer's information had been stolen.[130] It was thus

123. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) (holding that plaintiffs had no standing when there was no evidence that the "intrusion was intentional" nor that the hacker did anything but access the data).

124. *Id.* at 42.

125. *See id.* at 44 (differentiating the case from Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007)).

126. *Id.* at 42–43.

127. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

128. 794 F.3d at 693; *see also Galaria*, 663 F. App'x at 389 (quoting *Remijas*, 794 F.3d at 693).

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

130. *Id.* at 693–94.

plausible to infer that the *purpose* of the hack was to use the customer information.[131] The D.C. Circuit has used the same reasoning to argue that identity theft is the ultimate conclusion of a data breach of consumers' data.[132] This intentionality analysis in hacking cases has become the dominant trend among the circuits.

While other courts have presented different results,[133] no circuit has applied the intentionality analysis and denied standing in a hacking case. The circuit courts that have denied standing in hacking cases have instead focused largely on the second factor, the nature of the information.[134] For instance, in *In re SuperValu*, the Eighth Circuit did not attempt to reconcile its divergent result "because the cases ultimately turned on the substance of the allegations before each court."[135] The court instead held that some plaintiffs lacked standing because the theft of credit card information and the statistics cited by the plaintiffs about the risk of misuse did not generate a "substantial risk" of injury.[136] The Eighth Circuit's decision to focus on cited statistics rather than the intentionality analysis does not create a strong legal "split," but by ignoring the intentionality factor, the circuit court implicitly held that a thief intentionally targeting credit card information was not sufficient to create standing. The Eighth Circuit's decision—either ignoring the intentionality analysis or denying that an intentional hack created a "substantial risk" of misuse—clearly splits from the Seventh and D.C. Circuits.

The other circuits that have denied standing to data breach litigants who have not experienced misuse of their data have applied the intentionality analysis in a way that does not present a legal "split," despite creating divergent results. Recall that the Fourth Circuit case involved the theft of a laptop, not a hack in which a data thief targets a

131. *See id.* at 690, 693–94 ("At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach.").

132. *See Attias*, 865 F.3d at 628–29 ("No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

133. The cases from the Second and Eighth Circuits present the divergent results. *See In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 768–72 (8th Cir. 2017) (holding that there was not a substantial risk of future identity theft or fraud for the plaintiffs that had not yet experienced misuse); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017) (denying standing after customer data was hacked).

134. *See In re SuperValu, Inc.*, 870 F.3d at 766 (addressing credit card information, including card verification value (CVV)); *Whalen*, 689 F. App'x at 90 (addressing credit card data). Section II.B also addresses the nature of the information and provides more detail on why the nature of the information can affect the standing analysis.

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

136. *Id.* at 771–72.

consumer's information after bypassing security.[137] And the Third Circuit's case was not a true hacking case because the plaintiffs did not plead that their information was actually accessed by an unauthorized party.[138] Both of those cases require additional inferences—that the thief knew how to access the data on the laptop and would do so rather than sell the laptop as expensive hardware and that the hacker accessed the data and downloaded it without leaving a trace. The necessity of those inferences diminishes the intentionality of the breach and weakens the overall chain of inferences leading to the ultimate harm, making the risk of identity theft too speculative.[139]

Despite the apparent clarity in the circuits about the application of the intentionality factor (when it is applied), there is a strong argument that its application remains flawed. By ignoring the intentionality analysis and deciding on general statistics, the Eighth Circuit missed an opportunity to expand on the Fourth Circuit's analysis in *Beck*.[140] Without clear direction on what is considered sufficiently "imminent," courts are trying to discern what is "substantial" under *Clapper*. But the Sixth, Seventh, and D.C. Circuits' logic—that a hack will "sooner or later" lead to misuse[141]—seems to ignore the reality of what happens to personal data after it is compromised through a hack.[142]

After a thief has copied the data, she need not use the data for identity theft immediately or even ultimately in order to profit.[143] Indeed, hackers can—and do—repackage information for sale on the dark web rather than go through the effort of trying to conduct identity

137. *See* Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) (distinguishing the physical theft case at bar from hacking cases).

138. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (distinguishing the facts at issue from other hacking cases where the plaintiff alleged that the data was "read, copied, and understood").

139. *See Beck*, 848 F.3d at 273–75.

140. *See id.* at 273–74.

141. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015); *see* Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) ("No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 389 (6th Cir. 2016) (quoting *Remijas*, 794 F.3d at 693).

142. Note a hack is distinct from a breach associated with the theft of physical records, but the same logic would apply as the thief must merely offload the information or digitize the records.

143. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [https://perma.cc/HZ4V-ZX96] (noting the range of prices that various data can fetch on the dark web).

theft themselves.[144] With this knowledge, the chain of inferences is filled with more and more possibilities, resting "on speculation about the decisions of independent actors."[145] Furthermore, there is every incentive to misuse the data quickly—before companies are aware of the breach and before consumers can put up precautions—decreasing the strength of each individual inference in the chain of actors as a case drags on.[146]

Inferring the intent of third parties also seems to be the exact sort of speculation that the Court cautioned against in *Clapper*.[147] At times, the Court has allowed intent to establish standing and has even implied that an analysis of intent is appropriate to assess standing. But in those circumstances, the intent assessed was one of the parties—not a third party. Like in *Clapper*,[148] analyzing the intent of third parties primarily arises in cases in which plaintiffs are trying to establish the likelihood that the government will commit a specific act,[149] but the Court has also looked to the intent of plaintiffs to establish an injury in fact.[150] In a typical data breach case, however, the intent in question is that of a third party: the hacker (or her potential buyers).

In a world where "substantial risk" of future injury is the standard, however, courts must infer something about the future, necessarily implicating the actions of possible third parties. So while the Sixth, Seventh, and D.C. Circuits' explanation seemingly goes a bit too far under *Clapper*, this step of assessing intentionality is where

144. *See* Dion & Smith, *supra* note 20, at 263–66 (detailing the layout of the dark web and the steps that hackers go to in order to resell compromised data rather than use it for identity theft themselves).

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

146. *See* Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) (noting that the more time that passes, the more speculative injuries from breaches become); Robert Elgart, *The Data Black Market: Where Hackers Take Stolen Data*, TURN-KEY TECHS. (Aug. 5, 2019), https://www.turn-keytechnologies.com/blog/article/the-data-black-market-where-hackers-take-stolen-data/ [https://perma.cc/Y5QD-UTK2] (noting that this speed is particularly relevant for credit card theft).

147. *See Clapper*, 568 U.S. at 414 (noting that the Court has a "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors").

148. *See id.* at 407 ("[Plaintiffs] claim that there is an objectively reasonable likelihood that their communications will be acquired [by the government] at some point in the future, thus causing them injury.").

149. *See, e.g.*, City of Los Angeles v. Lyons, 461 U.S. 95, 105–06 (1983) (unsuccessfully trying to base standing on the intent of the police to continue using a chokehold policy).

150. *See* Susan B. Anthony List v. Driehaus, 573 U.S. 149, 159 (2014) (holding that a plaintiff can establish injury in fact via a threat of prosecution if the plaintiff "alleges 'an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute' " (quoting Babbitt v. Farm Workers, 442 U.S. 289, 298 (1979))). *Cf.* Lujan v. Defs. of Wildlife, 504 U.S. 555, 564 (1992) (" '[S]ome day' intentions—without any description of concrete plans, or indeed even any specification of *when* the some day will be—do not support a finding of the 'actual or imminent' injury that our cases require.").

circuits have to start when assessing the risk of future identity theft. The level of intentionality helps differentiate hacks where information was specifically targeted from those where the data was potentially incidental to another theft or hack.[151] A stolen laptop itself has value, decreasing the likelihood that the data was stolen for the purpose of identity theft—especially if the information was encrypted.[152] While inferences about a third party are necessary, and the circuits have not confronted the reality of the market for personal data, hacking cases do present fewer inferences than those made in *Clapper* because the bad act—the hack—has already occurred; it is not speculative like the surveillance in *Clapper*. Furthermore, *Clapper* formally applied a "certainly impending" standard rather than a "substantial risk" standard, meaning the number of contingencies that were impermissible in *Clapper* cannot be applied strictly to data breach cases.[153]

2. Nature of the Information

Another factor that contributes to the risk of imminent harm is the nature of the information disclosed. Primary personally identifying information—such as social security numbers, birth dates, driver's license numbers, or biomedical information—is distinct from certain financial information, like credit and debit card information.[154] And both of these types of information are more sensitive, and potentially more harmful, than other types of information that can lead to identifying an individual, such as names, street addresses, email addresses (without passwords), and phone numbers—information that is probably publicly available.[155] A victim can change a credit card

151. *Compare Beck*, 848 F.3d 262 (4th Cir. 2017) (stolen laptop and medical records), *and* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 532–33 (D. Md. 2016) (finding that there was no standing when the data breach only gave hackers access to email accounts, meaning that they did not target the personal information of patients when breaching the hospital employees' email accounts), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (conferring standing after a hack).

152. *Cf.* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (noting that the data on the stolen laptop was unencrypted).

153. *Clapper*, 568 U.S. at 401 (noting the application of the "certainly impending" standard).

154. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 30 (2007) [hereinafter GAO REPORT], https://www.gao.gov/new.items/d07737.pdf [https://perma.cc/85RM-VB9U] (explaining that personal information can be used to open new accounts or incur actual financial charges).

155. Alan McQuinn & Daniel Castro, *A Grand Bargain on Data Privacy Legislation for America*, INFO. TECH. & INNOVATION FOUND. 18 (Jan. 2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf [https://perma.cc/UG8G-PTC7] (noting that publicly available data is treated

number fairly easily,[156] but it is difficult, and sometimes impossible, to change a social security number or medical information.[157] These types of information may be accessed or stolen in a breach, and it is the release of these data together that presents the bigger issues. The black market for personal information on the dark web also indicates that data packages containing personal information, especially social security numbers linked with financial data, are more valuable, demonstrating a greater ability for use in identity theft and thus increasing the ultimate risk of identity theft.[158]

For standing purposes, canceling the compromised credit or debit card lowers the risk of identity theft because thieves cannot make fraudulent purchases with the now-canceled card information. This was the plaintiff's problem in *Whalen v. Michaels Stores, Inc.*, a case in which the plaintiff's payment card number and expiration date were compromised.[159] The plaintiff's alleged future injury was that her card information had been stolen, leading to two attempted uses, and that she thus faced a risk of future identity fraud.[160] The Second Circuit held that the plaintiff could not possibly face a threat of future fraud because the plaintiff had changed her card number after the theft and had pled "no specifics about any time or effort that she herself ha[d] spent monitoring her credit."[161] The Eighth Circuit has also explicitly held that compromised credit card information alone is insufficient to confer standing because no new accounts can be opened with just that information and because the risk of fraudulent charges is not "substantial."[162]

differently than other personally identifiable information by almost all privacy laws and privacy law proposals).

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

157. *See Can I Change My Social Security Number?*, SOC. SEC. ADMIN., https://faq.ssa.gov/en-US/Topic/article/KA-02220 (last modified Nov. 29, 2019) [https://perma.cc/GP3N-Q8T2] (detailing the steps required to change a social security number and noting that the Social Security Administration can only assign a new number after a breach if the data breach victim has actually suffered identity theft and "continues to be disadvantaged by using the original number").

158. *See* Ian Gray, *Pricing Analysis of Goods in Cybercrime Communities*, FLASHPOINT 2 (2019), https://www.flashpoint-intel.com/blog/a-look-at-the-pricing-of-cybercrime-goods-services/ [https://perma.cc/W8HW-D3NU] (detailing that "fullz"—the industry term for data sets that include name, social security number, date of birth, and account numbers together—typically cost between four and ten dollars in 2019—and potentially between thirty and sixty dollars if they include financial information).

159. 689 F. App'x at 89–90.

160. *Id.*

161. *Id.* at 90–91.

162. *See In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 768, 770–71 (8th Cir. 2017) (pointing to the 2007 GAO report, *supra* note 154, to show that only a few cases of card fraud actually resulted from data breaches from 2000 to 2005).

As articulated in *Whalen*, the Second Circuit's position on credit cards may create a perverse incentive. By the Second Circuit's logic, if the plaintiff had waited to change her credit card number until she had experienced the fraudulent charges, then she would have an injury in fact sufficient for standing.[163] This approach leaves little incentive for consumers to change their credit card number to prevent fraudulent charges, even though getting a new credit card number is the government- and industry- recommended response after a credit card breach.[164] *Clapper* teaches that plaintiffs cannot "manufacture standing."[165] But when plaintiffs responsibly follow expert recommendations to spend time changing a credit card number, they have suffered an "actual" loss, even if it is only nominal.[166] The mitigation costs incurred to prevent identity fraud are distinct from those in *Clapper* because unlike the government surveillance in *Clapper*,[167] the breach is not "hypothetical," and the perceived government and industry consensus on the reasonableness of mitigation costs demonstrates the legitimacy of the underlying harm. Perhaps that consensus even makes that harm "substantial."

In the previously discussed *In re SuperValu* case, the Eighth Circuit sided with the Second Circuit and held a data breach that compromises credit card information does not confer standing.[168] Like

163. *See, e.g.*, *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1023, 1027 (9th Cir. 2018) (holding that the plaintiffs had standing when part of the class experienced credit card fraud after a breach compromising "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information"); Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826, 829 (7th Cir. 2018) (holding that a plaintiff had standing after a bank took time to restore funds after a fraudulent charge).

164. *See* Brian O'Connor, *3 Things to Do if Your Credit Card or Debit Card Is Involved in a Data Breach*, EXPERIAN (Mar. 23, 2018), https://www.experian.com/blogs/ask-experian/3-things-to-do-if-your-credit-card-or-debit-card-is-involved-in-a-data-breach/ [https://perma.cc/67UK-4YKS] (industry recommendation); Lisa Weintraub Schifferle, *OPM Data Breach—What Should You Do?*, FED. TRADE COMMISSION: CONSUMER INFO. BLOG (June 4, 2015), https://www.consumer.ftc.gov/blog/2015/06/opm-data-breach-what-should-you-do?page=3 [https://perma.cc/VE4A-WDS9] (government recommendation).

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

166. For instance, in *Krottner*, two of the plaintiffs spent a "substantial" amount of time monitoring their bank accounts, and the court granted standing based on a risk of future injury. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141, 1143 (9th Cir. 2010). While documentation on the amount of time may be necessary to assess the extent of the damages, the point still stands that the loss is "actual," using the Court's language in *Lujan*. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 564, 564 n.2 (1992) (noting that after "actual" harm has been established, the "precise extent of harm" may be determined at trial).

167. *See Clapper*, 568 U.S. at 401–02, 410 (noting that the costs incurred by the plaintiffs were done so purely based on fear of surveillance).

168. *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 772 (8th Cir. 2017). One author has suggested that the Eighth Circuit's decision necessarily and correctly forecloses the risk of credit card fraud from being an injury in fact. *See* Jennifer Wilt, Note, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases*, 71 SMU

with all data breach cases, however, the facts and pleadings are important. The Eighth Circuit issued a narrow decision based on the statistics pled in the specific case;[169] the court's decision did not address credit card information theft more broadly. The Eighth Circuit based its decision on a Government Accountability Office ("GAO") report in the record that concluded only three of the twenty-four largest breaches from 2000 to 2005 resulted in some form of card fraud.[170] Unfortunately, the GAO's conclusions were not very strong, and the GAO has not conducted a subsequent study. The court and the report both noted that "[c]omprehensive information on the outcomes of data breaches is not available" and that the "extent to which data breaches result in identity theft is not well known."[171] The court also acknowledged that studies are not the only means of alleging a substantial risk of harm.[172]

The lack of empirical data on the likelihood of identity theft following a data breach is not unique to credit card information. Searching for empirical data to demonstrate substantial risk, plaintiffs have also cited studies suggesting that victims of a data breach are 9.5 times more likely to experience identity theft than the general population[173] and that between nineteen and twenty-five percent of data breach victims report suffering identity fraud.[174] Without providing guidance on what would be considered substantial, courts

L. Rev. 615, 619–20 (2018) (piecing together the GAO Report and *In re SuperValu, Inc.* to reach her conclusion). However, given the multiple disclaimers that the Eighth Circuit makes, that is a mischaracterization. Moreover, that argument would mean that even if a fraudulent charge—actual account fraud—occurred it would not suffice because the credit card company would reimburse the individual. *See id.* ("As the [*In re SuperValu, Inc.*] court noted . . . there is little risk of identity theft [based on stolen card information] because unauthorized accounts cannot be opened with credit card numbers alone. . . . [T]he only risk is fraudulent charges, which can often be easily remedied without court intervention." (footnote omitted)).

169. *In re SuperValu, Inc.*, 870 F.3d at 769 (specifically refusing to reconcile the case at bar with other circuits "because the cases ultimately turned on the substance of the allegations before each court").

170. *Id.* at 769–70; GAO REPORT, *supra* note 154, at 24.

171. *In re SuperValu, Inc.*, 870 F.3d at 771 (quoting GAO REPORT, *supra* note 154, at 5, 21).

172. *See id.* at 770 n.5 ("We recognize there may be other means—aside from relying on reports and studies—to allege a substantial risk of future injury, and we do not comment on the sufficiency of such potential methods here.").

173. Beck v. McDonald, 848 F.3d 262, 268, 275 (4th Cir. 2017) (noting that plaintiffs argued that their risk of identity theft was 9.5 times greater than before the breach and that thrity-three percent of "health-related data breaches result in identity theft").

174. *See* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) (citing the 9.5 times more likely statistic and noting that of those that received data breach notifications, nineteen percent reported identity fraud); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 877 (N.D. Ill. 2014) (applying—perhaps incorrectly—the "certainly impending" test and holding that Strautins did not demonstrate that identity theft is " 'certainly impending' for South Carolina taxpayers like herself").

have consistently denied that these statistics are sufficient to qualify as a substantial risk.[175]

Courts also note that because these statistics are general, they do nothing to address the risk that plaintiffs actually face.[176] Though these courts were all rendering decisions after *Clapper*, some of them[177] seemed to exclusively and inappropriately apply the "certainly impending" test, which should be reserved for rigorous standing inquiries involving separation of powers or national security, not assessing the standing of corporate data breach victims.[178] Even when the correct test is applied, however, plaintiffs would be better off not citing these general statistics at all because courts may use the statistics against them.[179]

Though the statistics do not create an apparent split, the sensitivity of credit card information does. Unlike the Second and Eighth Circuits,[180] the Seventh and Ninth Circuits have found that compromised credit card information can lead to a substantial risk of harm for those that have not yet experienced misuse.[181] The apparent split is (once again) not as clean as it seems, however. In the Seventh Circuit case, *Remijas*, plaintiffs pled that a significant number of credit

175. *See Khan*, 188 F. Supp. 3d at 533 (holding that the plaintiff's statistics are insufficient to support standing); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25–26 (D.D.C. 2014) (same); *Strautins*, 27 F. Supp. 3d at 877 (same).

176. *See, e.g.*, *Beck*, 848 F.3d at 275 n.7 (noting that the "9.5 times more likely" statistic does not address the specific facts of the case).

177. *See, e.g.*, *Khan*, 188 F. Supp. 3d at 533 (finding that the "general allegations" about the likelihood of identity theft were insufficient to establish that it was "certainly impending" and also holding that the statistics did not create a "substantial risk," without completely applying the "substantial risk" test); *Strautins*, 27 F. Supp. 3d at 876–77 (denying standing because "Strautins . . . failed to meet her burden to establish that identity theft is 'certainly impending' " even if the plaintiff was at a greater risk of identity theft after a hack that led to the theft of personal information).

178. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408–09 (2013) (noting that separation of powers questions merit an "especially rigorous" standing analysis and that the Court has often denied standing in cases involving intelligence and foreign affairs (quoting Raines v. Byrd, 521 U.S. 811, 819 (1997))).

179. *See In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 771 (8th Cir. 2017) (noting that the report cited by plaintiffs concludes that "most breaches have not resulted in detected incidents of identity theft") (citing GAO REPORT, *supra* note 154, at 21); *Beck*, 848 F.3d at 276 (concluding that a thirty-three percent risk of identity theft for breach victims is not "substantial").

180. *See In re SuperValu, Inc.*, 870 F.3d at 768–70 (holding that plaintiffs did not have standing when the thief had not yet used their compromised credit card numbers); Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 90 (2d Cir. 2017) (denying standing when the plaintiff had changed her credit card number before attempted misuse).

181. *See In re* Zappos.com, Inc. Customer Data Sec. Breach Litig., 888 F.3d 1020, 1023 (9th Cir. 2018) (holding that plaintiffs sufficiently alleged an injury in fact by alleging that credit card information was taken in the data breach); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015) (holding that plaintiffs adequately alleged standing when plaintiffs alleged that credit card information had been exposed in a data breach).

cards—9,200 of the 350,000 compromised cards—had been misused.[182] And in the relevant Ninth Circuit case, more than a dozen instances of identity theft were reported after a hack of Zappos.com led to compromised credit card information.[183] In contrast to those two cases, the Eighth Circuit plaintiffs in *In re SuperValu* pled that only one of them had suffered misuse post-breach,[184] and there was also only one instance of misuse in the Second Circuit case.[185] One instance of misuse is significantly different from the 9,200 that suffered post-breach abuse in *Remijas*,[186] and at least marginally different from the more than a dozen instances of misuse in the Ninth Circuit case.[187] These distinctions make it easier to reconcile the cases and avoid a quintessential "split" on whether compromised credit card information alone is sufficient to create a substantial risk. On the other hand, the factual differences in the cases make it difficult to conclude that credit card information alone—without any misuse of part of the compromised data, as was the case in the Seventh[188] and Ninth[189] Circuits—would be sufficient to create standing.

One other feature of stolen information plays an important role in the risk of identity theft post-breach: encryption. When data is encrypted, the hacker decrypting the data is an additional inference that the court must make to reach the ultimate identity theft.[190] This is particularly relevant in stolen records or stolen laptop cases in which data on the stolen device was unencrypted.[191] Lowering the likelihood

182. 794 F.3d at 690.

183. *See In re Zappos.com, Inc.*, 888 F.3d at 1027 (noting that other victims of the breach experiencing identity theft can support the contention that identity theft is possible—and thus that the likelihood of identity theft is higher); Brief of Appellants (Redacted) at 31-32, *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020 (No. 16-16860) (detailing the number of victims that had suffered financial losses).

184. 870 F.3d at 768.

185. *Whalen*, 689 F. App'x at 90.

186. 794 F.3d at 690.

187. *In re Zappos.com, Inc.*, 888 F.3d at 1027.

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

189. S*ee In re Zappos.com, Inc.*, 888 F.3d at 1027 ("[The misuse of some of the compromised credit cards] undermines Zappos' assertion that the data stolen in the breach cannot be used for fraud or identity theft."). This leads into the final factor that explains the results in the cases, a factor that I address in the next Section. To foreshadow a bit, because part of the compromised data had already been misused in the Ninth Circuit case, the inference that the rest of the data may be misused was easier to draw, increasing the risk of misuse. *Id.*

190. *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 24–25 (D.D.C. 2014) (denying that a substantial risk of harm existed and listing the decryption of the stolen data as a step in the chain of inferences necessary to infer future harm).

191. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (granting standing when laptops with unencrypted employee data were stolen), *with In re Sci. Applications Int'l Corp.*, 45 F. Supp. 3d at 25 (denying standing where data tapes that would have to be decrypted were among items stolen).

of standing based on responsibly encrypted data is an added incentive for companies to encrypt their data, which is an important step in limiting the overall likelihood of data breaches and any subsequent identity theft.[192]

To summarize, the circuits have properly noted that the sensitivity of data—depending on whether it is personally identifiable information, financial information, or already publicly disclosed—contributes to the risk of misuse. While there is apparent disagreement over whether compromised credit card information can create standing, no circuit has completely written off the prospect, and other factors—such as the cited empirical studies[193] or insufficiently precise pleadings[194]—may also explain the denial of standing in those cases. Either way, the point remains that social security numbers and other personally identifiable information have a higher risk of causing a plaintiff harm than the release of credit card information. Furthermore, some courts have noted that if one or more of the compromised credit cards is misused, then the likelihood of potential misuse of the rest of the compromised credit cards increases, creating a substantial risk of future harm.[195]

3. Proven Misuse of Only Some Victims' Data

The third factor used by circuits is evidence of misuse of some of the stolen data. Some circuits have allowed misuse of part of a compromised dataset to raise the risk that a victim's data will be misused, even if that victim's data is in a part of the compromised data that has not yet been misused.[196] As outlined above, however, the Eighth Circuit has held that even where one plaintiff can demonstrate fraudulent charges or attempted misuse sufficient to confer standing,

192. *See* Rick Robinson, *Three Lessons from the Target Hack of Encrypted PIN Data*, SEC. INTELLIGENCE (Jan. 9, 2014), https://securityintelligence.com/target-hack-encrypted-pin-data-three-lessons/ [https://perma.cc/N2DY-FY86] ("[E]ncrypted data thwarts the incentive to steal the data.").

193. *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 771 (8th Cir. 2017).

194. *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017):

> [Plaintiff] pleaded no specifics about any time or effort that she herself has spent monitoring her credit. Her complaint alleges only that "consumers must expend considerable time" on credit monitoring, and that she "and the Class suffered additional damages based on the opportunity cost and value of time that [she] and the Class have been forced to expend to monitor their financial and bank accounts."

(alteration in original).

195. *See In re* Zappos.com, Inc., 888 F.3d 1020, 1027–28 (9th Cir. 2018) (noting that if part of the compromised data set has been misused, then the probability of credit card misuse increases—a future injury that would require time and effort to prevent).

196. *Compare Krottner*, 628 F.3d at 1143 (finding standing), *with In re SuperValu, Inc.*, 870 F.3d at 768–72 (denying standing).

the risk of misuse is still insufficient for the remainder of the plaintiffs who cannot demonstrate misuse.[197] This is at odds with the Seventh and Ninth Circuits' holdings, which have allowed evidence of misuse by part of a plaintiff class to augment the risk of identity theft for the rest of the class.[198]

The Seventh and Ninth Circuits' position is more consistent with Supreme Court precedent, which allows a putative class to proceed if one named plaintiff has standing.[199] Confusingly, the Eighth Circuit acknowledged the precedent but then seemingly ignored it by refusing to find standing for the class.[200] Furthermore, the Eighth Circuit's analysis seems incomplete, even considering the GAO report it cites: if it is true that only a small number of data breaches do lead to account fraud, the presence of account fraud in part of the class would seem to suggest that this is the kind of breach that would lead to such harm.[201]

* * *

This Part demonstrated that the circuit "split" is not as much of a split as it seems. Much of the intentionality factor's apparent split can be explained by factual differences, particularly the demonstrated level of unauthorized access. Credit card information alone is less sensitive than other personally identifiable information and may not suffice to create standing. But misuse of part of the compromised credit card information can elevate the threat of credit card fraud to a substantial risk.

The third factor can also help create standing for plaintiffs who might lose out under the first factor if the Supreme Court decides to take a strict approach that leans against inferring the actions of third

197. *In re SuperValu, Inc.*, 870 F.3d at 769–70 ("With the exception of [one] plaintiff . . . the named plaintiffs have not alleged that they have suffered fraudulent charges on their credit or debit cards or that fraudulent accounts have been opened in their names.").

198. *See In re Zappos.com, Inc.*, 888 F.3d at 1027–28 (finding that risk of identity theft after hack of credit card records was sufficient to confer standing, and that the fact that part of class had experienced fraud raised the risk for the other part of the class); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015) (conferring standing based on future injury after a hack of credit card information and emphasizing that plaintiffs had alleged that "9,200 cards [had] experienced fraudulent charges *so far*"); *Krottner*, 628 F.3d at 1143 (conferring standing based on the threat of future identity theft after company laptop containing unencrypted personal information was stolen).

199. *See, e.g.*, Horne v. Flores, 557 U.S. 433, 446 (2009); Village of Arlington Heights v. Metro. Hous. Dev. Corp., 429 U.S. 252, 264 n.9 (1977).

200. *See In re SuperValu, Inc.*, 870 F.3d at 768 (citing *Horne*, 557 U.S. at 446; *Arlington Heights*, 429 U.S. at 264 n.9).

201. *See id.* at 769–71 (indicating that at least one named plaintiff alleged that they had suffered fraudulent charges on their credit card); *supra* notes 168–170 and accompanying text.

parties—a possibility suggested by *Clapper*.[202] In Section III.A, this Note explains how the Supreme Court could provide clarity to lower courts by enunciating positions on these factors and establishing a test for injury in fact for data breach cases. Specifically, the Court should (1) find that the mere fact of the breach *alone* is sufficient to demonstrate intentionality, (2) reject decade-old statistics on the likelihood of misuse of plaintiffs' information and assign import to the sensitivity of the breached information, and (3) side with the Seventh and Ninth Circuits and hold that demonstrated misuse of some of the information increases the risk of misuse for the rest of the victims.

B. Private Rights of Action Applied to Data Breach Litigation

Instead of arguing that the risk of future misuse is a substantial risk, a limited number of data breach victims can argue that a company injured them by violating a statute with a common law interest.[203] The Supreme Court's *Spokeo* decision made clear that not all violations of a statute suffice to create an injury in fact, even if the statute provides a private right of action.[204] Specifically, a mere procedural injury is not "legally cognizable,"[205] but the line between a mere procedural injury and a legally cognizable injury is a fine one. Breaking down the analysis into a number of steps is helpful.

Similar to the uncertainty surrounding the "substantial risk" test under *Clapper*, following *Spokeo*, federal courts try to divine whether Congress intended to create a concrete interest in a statute.[206] Then, if an interest is discerned, the court decides whether the plaintiff has alleged a violation of that interest.[207] If the plaintiff does not allege a violation of the interest intended by Congress, the plaintiff has one

202. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013) (commenting that the Court has a "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors").

203. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639–41 (3d Cir. 2017) (finding standing in a data breach suit based on congressional intent that the FCRA protect the same interest as common law privacy torts).

204. *See Spokeo I*, 136 S. Ct. 1540, 1549 (2016) ("Article III standing requires a concrete injury even in the context of a statutory violation.").

205. *See id.* ("[A plaintiff] could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.").

206. *See, e.g.*, *In re Horizon Healthcare Servs. Inc.*, 846 F.3d 625, 638–39 (analyzing the holding of *Spokeo* and concluding that Congress intended to confer standing to enforce violations of the FCRA).

207. *See* Dreher v. Experian Info. Sols., Inc., 856 F.3d 337, 346–47 (4th Cir. 2017) (identifying "ensur[ing] fair and accurate credit reporting, promot[ing] efficiency in the banking system, and protect[ing] consumer privacy" as the interests Congress intended to create in the FCRA and finding that the plaintiff had not sufficiently alleged that the statutory violation would make any difference to any of those interests (quoting Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52 (2007))).

more bite at the apple: the court will examine whether the statutory violation that the plaintiff is alleging has a sufficiently "close relationship" to a common law interest to rise to "legally cognizable" under *Spokeo*.[208] The private right of action in a statute then allows the individual to vindicate that interest at law.[209]

This chain of reasoning adds to the uncertainty for data breach litigants who have not suffered pecuniary damages because it relies heavily on the text of a statute—whether the statute covers the breached entity or the breached information,[210] whether the individual suing is under the class protected by the statutory interest and by the private right of action,[211] and whether the interest is "close" to one at common law.[212] These various steps demonstrate the possible pitfalls of trying to use a statutory private right of action to establish liability and may explain why relatively few data breach plaintiffs are able to successfully use private rights of action to establish standing.

Across the circuits, this process of identifying a statutory interest in order to confer standing has led to mixed results for plaintiffs. Some circuits have looked at the specific provisions in the Fair Credit Reporting Act that are cited by a plaintiff to determine whether those provisions create a statutory interest (a "legally cognizable interest") that the Act's private right of action allows

208. *See, e.g.*, *In re* Vizio, Inc., Consumer Privacy Litig., 238 F. Supp. 3d 1204, 1215–16 (C.D. Cal. 2017) (providing an overview of the history of privacy torts and finding that the claimed injury protected by the statutes at issue, the Video Privacy Protection Act and the Wiretap Act, was sufficiently close to the common law torts of "intrusion upon seclusion" and "disclosure of information in breach of a confidential relationship").

209. *Strubel v. Comenity Bank*, 842 F.3d 181, 186–90 (2d Cir. 2016), provides the archetype that other circuits, including the Ninth Circuit in *Spokeo II*, 867 F.3d 1108, 1113 (9th Cir. 2017), have followed when assessing whether a private right of action allows for an individual to vindicate a statutory right or whether the private right of action provision does not allow for the plaintiff to establish standing because the interest was merely procedural and not substantive.

210. The FCRA only covers consumer reporting. 15 U.S.C. § 1681e (2012). This leads to a gap in covering even data breaches of consumer reporting agencies. Perhaps one of the best examples of this gap in coverage came in litigation surrounding the Equifax breach. In one of the Equifax cases, a federal district court dismissed an FCRA claim because the information disclosed did not constitute a "consumer report," even though the information consisted of names, credit card numbers, social security numbers, dates of birth, driver's license numbers, credit addresses, and tax identification numbers. *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1308, 1313–14 (N.D. Ga. 2019).

211. *See* Enslin v. Coca-Cola Co., 739 F. App'x 91, 96 (3d Cir. 2018) (affirming dismissal of data breach suit because the claim fell outside of the statute of limitations in the private right of action); Kuhns v. Scottrade, Inc., 868 F.3d 711, 718–19 (8th Cir. 2017) (affirming dismissal of data breach suit because the statute only covered actions by businesses associated with a sale and required the plaintiff to suffer a pecuniary loss to fall within the protected class).

212. *See supra* Section II.

plaintiffs to vindicate through civil action.[213] Others have looked more broadly, however, at the overall purpose of the FCRA in assessing the statutory interest at stake.[214] The Ninth Circuit has even come out on both sides, sometimes finding that the statute creates a statutory right to information and sometimes finding that a statutory violation is merely procedural and requires a more concrete interest.[215]

The Third Circuit is the only circuit that has used the presence of a statutory private right of action in federal legislation to confer standing in a data breach suit.[216] In *In re Horizon*, the Third Circuit ruled that plaintiffs had standing when they alleged that the defendant had improperly "furnish[ed]" their information under the FCRA when a thief stole the defendant's laptops containing unencrypted personal information, including social security numbers.[217] The FCRA forbids the "unauthorized dissemination of personal information by a credit reporting agency," which the court found creates a right to privacy that has "traditionally been regarded as providing a basis for a lawsuit in English or American courts."[218] When addressing *Spokeo* on remand from the Supreme Court, the Ninth Circuit echoed the Third Circuit's holding: the private right of action in the FCRA allowed the plaintiffs to vindicate a right to privacy that the courts inferred from the statute.[219] Key to both of these post-*Spokeo* decisions was the courts' willingness to find a linkage between the common law privacy right and the interest Congress intended to protect.

However, not all courts have found a private right of action and a linkage to a common law privacy tort when examining federal legislation in data breach suits, demonstrating the lack of clarity existing for those trying to establish standing based on traditional privacy torts.[220] At the circuit level, the Third Circuit handed down its

213. *See, e.g.*, Robertson v. Allied Sols., LLC, 902 F.3d 690, 696 (7th Cir. 2018) (analyzing the statutory construction of the FCRA and concluding that the provisions in question were meant to serve substantive interests, not merely procedural ones).

214. *See* Dreher v. Experian Info. Sols., Inc, 856 F.3d 337, 346 (4th Cir. 2017) (holding that the plaintiff's cited interest did not match up with the broad purposes of the Act).

215. *Compare* Dutta v. State Farm Mut. Auto. Ins. Co., 895 F.3d 1166, 1175–76 (9th Cir. 2018) (denying standing after a plaintiff was not provided with sufficient opportunity to contest inaccurate credit information in violation of the Act), *with* Syed v. M-I, LLC, 853 F.3d 492, 499–500 (9th Cir. 2017) (conferring standing based on the right to information and privacy and no other concrete injury).

216. *See In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639–41 (3d Cir. 2017) (finding standing in a data breach suit based on congressional intent for the FCRA to protect the same interest as common law privacy torts).

217. *Id.* at 630–31, 641 (alteration in original).

218. *Id.* at 639–40 (quoting *Spokeo I*, 136 S. Ct. 1540, 1549 (2016)).

219. *Spokeo II*, 867 F.3d 1108, 1115 (2017).

220. *See, e.g.*, *Spokeo I* at 1549 ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a

decision in *Kamal v. J. Crew Group, Inc.*[221] and refined the definition of common law privacy torts just two years after seemingly expanding standing to cover most privacy torts in *In re Horizon*.[222] In *Kamal*, the plaintiff argued that Congress had contemplated the risk of identity theft when writing the Fair and Accurate Credit Transactions Act because the congressional record showed that experts recommended credit card numbers not be printed in full on receipts for fear of criminals getting their hands on them.[223] In *In re Horizon*, the Third Circuit found a sufficiently "close relationship" between the common law privacy tort of unreasonable publicity and the plaintiff's claim under the FCRA because both were meant to protect against the "improper dissemination of information."[224] However, the *Kamal* court found that the injury in common law privacy torts, including in breach of confidence cases, involved the dissemination of personal information to a third party.[225] The court held that Kamal could not demonstrate that a third party had access to his information because the violation was merely putting additional digits of his credit card number on a receipt; thus, his claim failed because his injury under FACTA did not bear a "close relationship" to a common law action.[226] In contrast, the Eleventh Circuit has spelled out an argument that there *is* a sufficiently "close relationship" between the injury meant to be prevented by FACTA and a common law breach of confidence claim.[227]

These FACTA and FCRA claims, which involve intentional disclosures in violation of statutes, are not data breach claims. But courts' analysis of what constitutes a statutory interest and what constitutes a "close relationship" between a statutory interest and the common law interest will have bearing on future data breach litigation if Congress decides to create a private right of action in comprehensive privacy legislation. Federal circuit courts will also impact future data breach litigants if courts that are less receptive to arguments about future harm face similar FCRA claims to the ones in *In re Horizon*.

statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.").

221. 918 F.3d 102 (3d Cir. 2019).

222. *Compare id.*, at 114 (noting that third party access is required to prove a close relationship with privacy torts), *with In re Horizon*, 846 F.3d at 638–39 ("And with privacy torts, improper dissemination of information can itself constitute a cognizable injury.").

223. 918 F.3d at 102, 115 n.5, 116 (2019).

224. 846 F.3d at 638–39.

225. 918 F.3d at 114.

226. *Id.*

227. Note that the argument is merely illustrative because as of now, the court is waiting to hear the case en banc and has vacated the previous rulings detailing this argument. *See* Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175, 1191–92 (11th Cir. 2019), *reh'g en banc granted*, *opinion vacated*, 939 F.3d 1278 (11th Cir. 2019).

Furthermore, the inconsistent outcomes arising from varied readings of a given statutory interest demonstrate the importance of clearly defining the statutory interest that the private right of action is meant to protect.

States offer helpful examples on how to formulate a federal data breach statute that may be able to confer standing, even for plaintiffs seeking standing based on a violation of data breach notification statutes. Data breach notification violations sound in procedure more than other standing arguments based on an increased risk of harm or broad violation of the right to privacy.[228] Therefore, *Spokeo*'s admonishment that "bare procedural violations" do not suffice to create standing makes it particularly hard for plaintiffs to establish standing to enforce data breach notification statutes.

Many states that include private rights of action in their data breach laws require a demonstration of "actual damages" in order to enforce statutory violations through a private right of action. As documented in Section II.A, many data breach victims cannot yet demonstrate "actual damages," forcing them to argue that there is a substantial risk of future harm. Requiring "actual damages" makes it nearly impossible to privately enforce data breach notification, which will only become more important as more and more consumers are affected by data breaches.[229]

One scholar has documented the emphasis that state legislatures put on notification statutes and argues that refusing to honor a private right of action in a notification statute by denying standing defeats the legislative intent of those statutes.[230] Her argument's existence is telling: the private rights of action and the statutory text in many state statutes may not sufficiently convey the legislative intent of their authors. Even California's new privacy law, the California Consumer Protection Act, may not go far enough to incentivize notification because it allows for public enforcement only by the attorney general.[231]

228. *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014) (conferring standing based on the increased risk of harm, which also satisfied to create an additional concrete interest to confer standing based on a statutory interest, but still denying standing based on a failure to show a cognizable injury arising from a possible statutory violation of the data breach notification provision).

229. *See* Press Release, Sen. Bob Menendez, What You Should Know About Equifax Data Breach (Sept. 14, 2017), https://www.menendez.senate.gov/news-and-events/press/what-you-should-know-about-equifax-data-breach [https://perma.cc/RR4R-6U4R] (noting that it was "outrageous" for Equifax to wait more than a month to inform consumers of a breach).

230. *See* Elliott, *supra* note 72, at 242–47.

231. *See* CAL. CIV. CODE § 1798.150-155 (West 2020) (allowing individuals to get statutory damages, but reserving enforcement of other violations of the Act, including the unreasonable delay provisions, for the Attorney General).

III. SOLUTIONS

This Note proposes two approaches that would independently eliminate much of the uncertainty for data breach plaintiffs and defendants. First, the Supreme Court should adopt a multifactor test for assessing whether the risk of misuse—through either identity theft or payment card fraud—is substantial after a breach. Second, Congress should solve the standing issue by including in federal legislation that victims have a "legally cognizable interest" that they can defend through a statutory private right of action.

A. The Supreme Court Steps In

The Supreme Court should help clarify the divergent results by establishing a test focused on intentionality, the nature of the compromised data, and whether any of the victims of the breach have had their data misused. As mentioned in Part II, the divergent results and the various splits are heavily fact-dependent, which can make standing in data breach cases difficult to analyze, but the injury-in-fact inquiry inevitably requires heavy analysis of case facts. It is also difficult to imagine one case that would allow the Supreme Court to create a universal test resolving all uncertainty in the sphere of data breach litigation. But if such a case were to arise, this Note proposes a three-factor test that would help the Court and litigants wade through the facts to reach common ground on standing.

The first factor, intentionality or targeting, would examine the level of sophistication of the breach, as well as other evidence demonstrating an intent to take the plaintiff's information. Under the current circuit analysis, opinions on both sides of the divergent results can be reconciled with this approach. The Fourth Circuit properly denied standing in *Beck* when a laptop was stolen because there was a lack of intent to commit identity theft,[232] while the D.C. Circuit properly conferred standing when there was evidence that the Chinese government—a sophisticated and potentially malicious party—was responsible for a hack in *In re OPM*.[233] The D.C. Circuit's approach does not expand standing to include all breaches that occur by hacking; if a plaintiff cannot demonstrate that a hacker penetrated and copied personal information, then she may not be able to show sufficient intent.[234] A test that grants standing at the moment of a breach—

232. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

233. *In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 56 (D.C. Cir. 2019).

234. *See* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 532–33 (D. Md. 2016) (finding that there was no standing when the data breach only gave hackers access to email

independent of the information collected and the conduct involved—would be in violation of *Clapper*'s instruction to examine "concrete facts."[235] While the application of this factor may seemingly contravene *Clapper*'s directive not to assess the decisionmaking of "independent actors," it does not because the test still relies on the plaintiff(s) properly pleading her case with sufficient facts to demonstrate intentionality.[236]

The second factor would focus on the nature of the information disclosed, allowing courts to reject claims based on the sensitivity of the stolen information. While credit cards may be less valuable to a data thief than personally identifiable information and may only lead to reimbursable fraudulent charges, the prospect of those charges should be enough to confer standing.[237] The main difference between credit card data and other, more sensitive types of data is that the consumer will have to take fewer steps to resolve the issue on the back end, but the risk of injury is looking at the likelihood of injury, not the level of damage to the consumer. Further, incurred mitigation costs could also qualify as a concrete injury if they were incurred based on government- and industry- recommended steps for victims to take in the wake of a breach.[238]

By including encryption in the analysis, the test will also incentivize companies to further encrypt their data, which will help reduce data breaches and the likelihood of identity theft after any breach.[239] Encryption plays a role in both the intentionality factor and the nature of the information factor because at least one court has already used evidence of successful decryption of compromised information to demonstrate the sophistication of the hacker, increasing

accounts, meaning that they did not target the personal information of patients when breaching the hospital employees' email accounts).

235. This is essentially what the *Remijas* logic, which assumes that the hacker wants to commit identity theft, would necessitate. *See* John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 955–56 (2016) (arguing that the Supreme Court should adopt the *Remijas* logic because malicious intent is enough to demonstrate a "substantial risk" of identity theft).

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

237. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015) (conferring standing when part of the class had experienced fraudulent charges after a hack).

238. *See id.* at 692. Note that this is not an argument that the underlying harm is substantial because the government and industry recommend steps. This is an argument that the government and industry should not be able to foist the cost of mitigation on consumers after a breach.

239. *See* Rick Robinson, *The Impact of a Data Breach Can Be Minimized Through Encryption*, SEC. INTELLIGENCE (Oct. 21, 2014), https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/ [https://perma.cc/R9BK-555J] (noting that encryption with a properly separated encryption key can reduce the value of data, disincentivizing any actual theft).

the likelihood of eventual identity theft.[240] Prioritizing the incorporation of encryption into analysis also represents low-hanging fruit given the relatively low rate of encryption across industries.[241]

Finally, if there is evidence of misuse or attempted misuse of any of the compromised data, it should further contribute to the substantiality of the risk of identity theft.[242] Opponents of conferring standing on data breach litigants who have not yet suffered identity theft often point to the numbers on the percentage of data breaches that result in identity theft.[243] But where part of the class can already demonstrate that malicious actors have used or tried to use part of the compromised data, there is a logical inference that the risk of identity theft increased for a given victim of that breach. This final factor should be evaluated only with the other two. By drawing out these three factors, it is clear there is less conflict among the circuits than some have suggested.[244]

B. A Federal Private Right of Action in Privacy Legislation

As a second, independent legislative proposal, Congress should step in and remove uncertainty for data breach plaintiffs. This legislative proposal takes a page from California's Consumer Privacy Act, which became effective at the start of this year.[245] A federal statute seeking to have data breach victims at least get past the standing stage must be properly constructed so that a data breach—even if

240. *See In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014) (holding that the hackers' deliberate targeting of the servers and their ability to use the defendant's own decryption software contributed to make the danger of misuse "certainly impending").

241. *See* 2019 THALES DATA THREAT REPORT GLOBAL EDITION, THALES 20 (2019), https://www.thalesesecurity.com/2019/data-threat-report [https://perma.cc/9LRP-BKT4] (surveying 1,200 executives that handle IT and data security across the globe and finding that "[f]ewer than 30% of enterprises say they use encryption for the vast majority of use cases studied, including disk encryption within datacenters, from cloud providers, in big data environments, in databases, within mobile devices, and in IoT environments").

242. *See In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020, 1027–28 (9th Cir. 2018) (finding that evidence that hackers took over plaintiffs' email accounts supported plaintiffs' "contention that the hackers accessed information that could be used to help commit identity fraud or identity theft").

243. *See, e.g.*, *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 768–71 (8th Cir. 2017) (relying on the 2007 GAO Report that found that only four out of twenty-four data breaches from 2000 to 2005 had resulted in identity theft).

244. *See* George Lynch & Adam Cooke, *Considering Standing Law and Future Risk of Harm in Data Breach Litigation*, BLOOMBERG LAW (Feb. 23, 2018, 12:37 PM), https://news.bloomberglaw.com/business-and-practice/considering-standing-law-and-future-risk-of-harm-in-data-breach-litigation [https://perma.cc/CF3A-6KYA] (arguing that the Sixth and Seventh Circuits positions are particularly irreconcilable with those that deny standing).

245. CAL. CIV. CODE § 1798.150 (West 2020).

inadvertent—implicates an invasion of privacy based on a "close relationship" to a traditionally recognized harm.[246] Such harms that have "traditionally been regarded as providing a basis"[247] for a common law action include a range of privacy torts, such as the unreasonable intrusion upon seclusion, appropriation of another's name or likeness, unreasonable publicity given to another's private life, and publicity that unreasonably places another in a false light.[248] Because merely a "close relationship" is required, a perfect analog is likely not necessary; the underlying concern of common law privacy torts—the inability of an individual to control her personal information[249]—would likely suffice to create "an invasion of a legally protected interest which is concrete and particularized and actual or imminent."[250]

Borrowing from both the *In re Horizon* court's finding that the FCRA's private right of action was meant to allow plaintiffs to protect against "unauthorized dissemination of personal information by a credit reporting agency"[251] and California's private right of action,[252] a narrow federal statute could define the scope of the private right of action by writing that it is meant to "protect against the unauthorized

246. *See Spokeo I*, 136 S. Ct. 1540, 1549 (2016) ("[I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit.").

247. *Id.*

248. Long v. Se. Pa. Trans. Auth., 903 F.3d 312, 324 (3d Cir. 2018) (citing RESTATEMENT (SECOND) OF TORTS § 652A(2)(a)-(d) (1977)); *see* DAVID A. ELDER, PRIVACY TORTS § 1:1 (2016) ("[T]he privacy torts have become well-ensconced in the fabric of American law." (footnotes omitted)). Note that breach of confidence is another possible common law action that may have a close relationship with the unauthorized disclosure of information. *See* Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 619–24 (2018) (arguing that the mere disclosure of another's information given in confidence, not the misuse or publication of that information, sufficed to create a harm at common law). *But see* Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114–15 (3d Cir. 2019) (holding that breach of confidence required the party violating confidence to have shown the information to a third party, a fact that is not always readily available to data breach victims).

249. *Long*, 903 F.3d at 324.

250. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992); *see In re* Horizon Healthcare Servs. Data Breach Litig., 846 F.3d 625, 639–40 (3d Cir. 2017) (noting that it is not necessary for a given claim to be an exact match for a common law cause of action, as long as the interest that Congress wanted to statutorily protect is the same injury as the one protected by the common law action).

251. 846 F.3d at 639.

252. *See* CAL. CIV. CODE § 1798.150 (West 2020):

> Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action . . . .

access and exfiltration, theft, or disclosure of a consumer's nonencrypted and nonredacted personal information."[253]

This proposed language is versatile enough to fit in a gambit of consumer protection statutes, so even if a comprehensive data privacy bill is unlikely, Congress could still continue expanding coverage piecemeal by inserting this language in other bills covering consumers. Assuming Congress adopted this language, however, the courts would still have to make the connection between the common law privacy torts and the interest created by Congress.

The Third Circuit's analysis in *In re Horizon* provides an illustration of how a court would analyze such a private right of action in federal legislation,[254] and the circuit's interpretations of FACTA's private right of action serve as a cautionary tale for drafters. To ensure the private right of action's proper breadth, it is important for drafters to clearly link the interest that the private right of action is meant to vindicate with the interest protected by a traditionally recognized common law cause of action.[255] The Third Circuit's analysis in *Kamal* shows the importance of explicitly spelling out the acceptable chain of inferences necessary to create a concrete injury. There, the plaintiff argued that the defendant had violated FACTA by including more digits of a credit card on a receipt than the statute allowed.[256] The defendant had plainly violated that statutory requirement, but the *Kamal* court refused to grant standing partially because the plaintiff's injury was not

253. Notably, the proposed language does not include any restrictions on what kind of data breaches may lead to a viable action because the focus of this Note is to provide possible solutions to the standing hurdle and does not address what statutory language would be necessary to ensure that victims are fairly compensated. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634, 637–39 (7th Cir. 2007) (holding that the plaintiff had standing to sue based on identity theft as a future harm but that the increased risk of identity theft was not "compensable"). Statutory damages may be one way to ensure compensation; as of January 1, 2020, California became the first state to allow consumers whose information has been compromised to recover statutory damages to compensate for a breach, even in the absence of actual damages. CAL. CIV. CODE § 1798.150 (West 2020).

254. *See* 846 F.3d at 638–39 (walking through how a breach creates an invasion of privacy similar to the tort of unreasonable publicity).

255. *Compare* Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114–15 (3d Cir. 2019) (holding that even under FACTA, which includes a private right of action, the common law action of breach of confidence required disclosure to a third party and that absent facts demonstrating such a disclosure, there was no intangible injury sufficient to survive *Spokeo*), *with* Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175, 1191–92 (11th Cir. 2019) (taking issue with how "close" the Third Circuit asserted that the common law action had to be to the present action and holding that a common law breach of confidence action protected against the same injury that Congress was trying to prevent with FACTA).

256. *Kamal*, 918 F.3d at 106.

sufficiently "close" to any common law privacy torts.[257] The court determined the traditional privacy torts were rooted in a third party gaining access to a plaintiff's personal information, and unlike in *In re Horizon*, there was no allegation that anyone else had seen the plaintiff's information.[258] If other courts follow the Third Circuit's lead, then plaintiffs who allege a breach—but cannot demonstrate that their specific information was accessed[259]—may be unable to vindicate a given private right of action if Congress does not clearly state the interest that the statute is meant to protect and how that interest links to the common law. These two Third Circuit cases show the importance of properly wording a statute by directly linking the concrete interest a data breach statute seeks to protect—whether that is the right to information or the right to privacy[260]—with the private right of action itself.

While few states create a private right that would explicitly allow a plaintiff to sue in the absence of actual damages, California's CCPA serves as an example of how a legislature could do so.[261] Congressional drafters would be wise to learn from state statutes that are less than explicit in whether they allow private enforcement. For instance, Iowa's data breach notification statute is geared towards enforcement by the Iowa Attorney General,[262] but it also states "[t]he rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under the law."[263] This ambiguity about private enforcement is not unique to Iowa.[264] And this again places courts in a position of determining whether a private

257. *Id.* at 114–15. The court also refused to grant standing because it determined that FACTA was meant to protect against actual identity theft rather than just the risk of identity theft. *Id.* at 115–16.

258. *Id.*

259. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing plaintiff alleged only that the defendant's system, which contained personal and financial information on employees, had been accessed, not that the information had been "read, copied, and understood").

260. *See* Syed v. M-I, LLC, 853 F.3d 492, 499–500 (9th Cir. 2017) (conferring standing based on a right to information and a right to privacy rooted in the FCRA).

261. *See* CAL. CIV. CODE § 1798.150 (West 2020); *see also, e.g.*, LA. STAT. ANN. § 51:3075 (2019) (allowing for a civil action to recover "actual damages" resulting from a failure to disclose a breach in a "timely manner"); S.C. CODE ANN. § 39-1-90 (2013) (allowing residents to sue to recover "actual damages" resulting from a negligent violation of the statute).

262. *See* IOWA CODE § 715C.2 (2018) (prescribing that "the attorney general may seek and obtain an order that a party held to violate th[e] section pay damages to the attorney general on behalf of a person injured by the violation").

263. *Id.* § 715C.2(9)(b).

264. *See, e.g.*, *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014) (classifying Colorado, Delaware, Iowa, Kansas, Michigan, and Wyoming data breach statutes as ambiguous as to private enforcement mechanisms).

right of action exists, while plaintiffs are faced with additional uncertainty as to whether their claim will even get past a motion to dismiss.[265] This burden on courts can be significant, especially if plaintiffs follow the example of recent litigants' cases after large breaches and allege a violation of over thirty states' statutes at a time.[266] Therefore, though it is less than ideal because it continues to contribute to the patchwork of data breach notification, states like Iowa could also adopt this Note's proposed language and create more explicit private rights of action as a way of providing clarity to courts and litigants.

Notably, even California's CCPA may come up short in incentivizing effective notification because it relies on limited public resources rather than private enforcement. Attorneys General have a range of mandates, but private parties are properly incentivized to ensure that companies adequately notify consumers. Moreover, granting the FTC additional authority to oversee broad enforcement of a data breach notification may not even suffice given the FTC's myriad mandates and resource constraints.[267] Any federal statute should not only follow California in allowing for a private right of action, but must also clarify that injuries that may seem procedural are clearly linked to a specific concrete interest in order to provide clarity to courts and to ensure victims can help enforce statutory violations.

CONCLUSION

In the absence of a federal statute and Supreme Court action, federal privacy law stagnates, detrimentally affecting consumers on a variety of levels.[268] This Note proposes a test that would provide guidance to the circuit courts on how to properly analyze standing in data breach litigation and also to the U.S. legal community on how the

265. *Compare In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295 (N.D. Ga. 2019) (allowing a private claim under the Wisconsin data breach notification statute to survive motion to dismiss when the court used statutory interpretation to conclude that the Wisconsin data breach statute was silent as to whether a private right of action exists), *with* Fox v. Iowa Health Sys., 399 F. Supp. 3d 780, 800 (W.D. Wis. 2019) (granting a motion to dismiss after finding that the Wisconsin data breach statute did not create a private right of action).

266. *See In re Target*, 66 F. Supp. 3d at 1158 (alleging a violation of thirty-eight states' data breach notification statutes).

267. *See* Chris Jay Hoofnagle, Woody Hartzog & Daniel Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress,* BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/LY62-XD2D] (noting that increased funding for the FTC is essential even absent any expansion in its statutory authority).

268. *See* Richards, *supra* note 19, at 1464 (noting the federal government's lag in confronting the changes that technology and big data have imposed on society).

Court will assess future injuries in general. The test focuses on the facts underlying a data breach. As an added institutional competence benefit, grappling with those facts would also help update the Court's privacy knowledge—and as a result, its jurisprudence. In a world of judicial inaction, Congress can also take steps to provide data breach victims with firmer ground to stand on by creating a concrete interest in a federal data breach statute that includes a private right of action. The statute should make clear that consumers have a right to know about any breach in a reasonable amount of time and that the private right of action is meant to protect that right. If the statute is unclear about what right it is meant to protect, Congress's desired outcome will be left up to judicial interpretation about what common law right a given statute is meant to protect—possibly leading to further complications at the standing stage.

Return to the woman who bought groceries with her credit card. As it stands, she faces extreme uncertainty in the wake of the breach,[269] and she can expect little help from the federal government. She must first assess what circuit she should file in, then she has to determine whether she falls within a state's private right of action or within one of the few federal statutes that contain a private right of action—and this is just the legal uncertainty. Though some companies offer credit monitoring services for a given period of time after a breach, plaintiffs typically pay—with their time or with their money—for any costs associated with changing their information, which amounts to an added cost of uncertainty. This Note confronts the uncertainty these data breach litigants face, and by taking up either of the proposed solutions, the federal government can provide much needed clarity and remove some of that uncertainty.

Devin Urness[*]

269. Solove & Citron, *supra* note 13, at 750–54 (discussing the harms that come from that uncertainty, including the increased-risk-of harm, costs associated with preventing harm, and anxiety).

* J.D. Candidate, 2020, Vanderbilt University Law School; B.S., 2014, Georgetown University, School of Foreign Service. I want to thank everyone who contributed to the development of this Note. Thanks to Judge Joe Brown, who helped me discover the issue and hone my writing, and thanks to Professor Kevin Stack for providing early advice on narrowing the topic. I cannot thank my peers on *Vanderbilt Law Review* enough. This Note would be nothing without their valuable insights and consistent diligence. I particularly want to thank Greg Maczko, Molly Dillaway, Patrick Perrier and the cite-checking team, Emily Sheffield, and Alicia Hoke, who was a constant source of encouragement.