Missouri Law Review

Volume 84
Issue 1 *Winter 2019*

Article 14

Winter 2019

The Eighth Circuit Further Complicates Plaintiff Standing in Data Breach Cases

Aaron Wynhausen

NOTE

The Eighth Circuit Further Complicates Plaintiff Standing in Data Breach Cases

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

Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017)

*Aaron Wynhausen**

I. INTRODUCTION

Mass data breaches are a symptom of the digital era and occur with increasing frequency. In the past decade, nearly every sector of the economy has experienced a major breach of personal data, including finance, healthcare, retail, government, hospitality, media, and technology.[1] Breaches affect consumer data, government agencies, voting rolls, healthcare providers, scientific data, business records and trade secrets, attorney work-product, and nearly everything else digital.[2] Fiascos surrounding poor data stewardship at companies, like Facebook and Equifax, are frequently featured in national media.[3]

As large data caches containing sensitive personally identifiable information continue to expand, the chances for a breach grow in kind. The potential harm from a breach varies depending on the type of data compromised. Breaches of the most sensitive data, such as social security numbers, embarrassing personal information, medical information, and bank account information, can lead to mass disruptions in people's lives. Breaches of less sensitive data, such as credit card information, online account login credentials, email addresses, home addresses, and phone numbers have less potential for

---

* J.D. Candidate, University of Missouri School of Law, 2019. Thank you to Courtney Lock, Lauren Vincent, David Rogers, Connor Smith, and Professor Dennis Crouch for their edits and comments to this Note.

1. *See, e.g.*, BAKERHOSTETLER, IS YOUR ORGANIZATION COMPROMISE READY?: 2016 DATA SECURITY INCIDENT RESPONSE REPORT 1–2 (2016), https://www.bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf.

2. *See, e.g.*, *id.* at 2.

3. *See, e.g.*, Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html; Brian Fung, *Equifax's Massive 2017 Data Breach Keeps Getting Worse*, WASH. POST (Mar. 1, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/.

direct harm but can have frustrating consequences for those whose data is compromised. No uniform federal law exists governing the legal duties of those who collect and store personally identifiable information ("PII"), and when a breach occurs, the difficulty in identifying actual harm or quantifying a remedy makes the appropriate legal response unclear.

In 2016, reported data breaches increased to a record 1,093 incidents – exposing over thirty-six million identified records.[4] Some estimates suggest that between eighty to ninety percent of Fortune 500 companies and government agencies have experienced a data security breach.[5] The proliferation of data breaches led one federal judge to note that "[t]here are only two types of companies left in the United States[] according to data security experts: 'those that have been hacked and those that don't know they've been hacked.'"[6] Influential digital security expert Brian Krebs summed up the phenomenon in a blog post identifying the "immutable truths" about data breaches:

> There are some fairly simple, immutable truths that each of us should keep in mind, truths that apply equally to political parties, organizations and corporations alike: [(1)] If you connect to the Internet, someone will try to hack it. [(2)] If what you put on the Internet has value, someone will invest time and effort to steal it. [(3)] Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it. [(4)] The price he secures for it will almost certainly be a tiny slice of its true worth to the victim. [(5)] Organizations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cybercrooks can expect to eventually be relieved of said assets.[7]

Plaintiffs have brought hundreds of class action lawsuits against organizations that were responsible for maintaining customer PII and subsequently suffered a breach.[8] While data breach cases have been litigated in nearly every

---

4. IDENTITY THEFT RES. CTR., DATA BREACH REPORTS: 2016 END OF YEAR REPORT 4 (2017), http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf.

5. Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1368 (2013).

6. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015) (quoting Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES: BITS (Apr. 22, 2013, 9:10 PM), http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/).

7. Brian Krebs, *Krebs's Immutable Truths About Data Breaches*, KREBS ON SECURITY (Jan. 9, 2017), https://krebsonsecurity.com/2017/01/krebss-immutable-truths-about-data-breaches/.

8. *See, e.g.*, Hayley Tsukayama, *Equifax Faces Hundreds of Class-Action Lawsuits and an SEC Subpoena over the Way It Handled Its Data Breach*, WASH. POST (Nov. 9, 2017), https://www.washingtonpost.com/news/the-

federal circuit court, each circuit has treated them differently with respect to standing and whether a claim for damages exists.[9] Most of these cases are appealed on standing issues.[10] This Note examines two recent cases from the U.S. Court of Appeals for the Eighth Circuit and analyzes how these decisions fit into the greater scheme of data breach litigation in the United States today.

II. FACTUAL BACKGROUND

This Note examines two cases from the Eighth Circuit, both dealing with the same general issue – an unauthorized breach of consumer data. Each class action was consolidated to a district court within the Eighth Circuit, dismissed for lack of standing, and appealed by the plaintiffs to separate panels.[11] The appellate decisions were released just nine days apart.[12] The type of breach was unique in each case, and the plaintiffs claimed different types of injuries, but the legal issue on appeal remained the same – did the plaintiffs sufficiently allege an injury in fact for purposes of establishing Article III standing? This Part summarizes the facts and provides a brief procedural history of each case.

A. Kuhns v. Scottrade, Inc.*: Decided August 21, 2017*[13]

The first of the two cases decided by the Eighth Circuit involved hackers accessing the customer database of Scottrade, a securities brokerage firm headquartered in St. Louis, Missouri.[14] Between September 2013 and February 2014, the hackers acquired PII of over 4.6 million customers.[15] The hackers then used this data to operate a stock manipulation scheme, a dozen illegal internet gambling websites, and even a Bitcoin exchange.[16] Scottrade was unaware of the breach until August 2015, when the Federal Bureau of Investigation ("FBI") notified Scottrade that the breach had occurred.[17] Scottrade began notifying affected customers through email and mail on October 2, 2015, and suggested customers be "vigilant" for signs of fraud for the next two years.[18] Scottrade then arranged to have customers receive one year of "identity repair

switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/.

9. *See* discussion *infra* Part III.

10. *See* discussion *infra* Section III.A.

11. *See In re* SuperValu, Inc., 870 F.3d 763, 765 (8th Cir. 2017); Kuhns v. Scottrade, Inc., 868 F.3d 711, 714 (8th Cir. 2017).

12. *See In re SuperValu*, 870 F.3d at 763; *Kuhns*, 868 F.3d at 711.

13. 868 F.3d at 711.

14. *Id.* at 713.

15. *Id.* at 713–14.

16. *Id.* at 714.

17. *Id.* at 715.

18. *Id.*; Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *1 (E.D. Mo. July 12, 2016), *aff'd sub nom.* Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017).

and protection services 'with no enrollment required'" and offered one year of free credit monitoring and identity theft insurance.[19]

When customers signed up for an account with Scottrade, they provided PII in the form of names, addresses, social security numbers, tax identification numbers, telephone numbers, email addresses, employer information, and work history.[20] A "Privacy Policy and Security Statement" was included in the agreement made with customers.[21] In the Privacy Policy, Scottrade claimed that it would "maintain physical, electronic and procedural safeguards . . . to guard . . . nonpublic personal information" and that it "offer[ed] a secure server and password-protected environment . . . protected by . . . encryption."[22] Scottrade also made two separate representations online that contained similar language.[23]

After the announcement of the breach, several customers ("Plaintiffs," collectively) filed four separate punitive class action complaints in three federal district courts.[24] The U.S. District Court for the Eastern District of Missouri consolidated the actions into its jurisdiction.[25] The four named Plaintiffs filed a consolidated class action seeking a certification of the class, damages for ten causes of action,[26] injunctive relief, and attorneys' fees and costs.[27] The district court refused to consider the merits of the case and dismissed the case without prejudice for lack of subject matter jurisdiction.[28] The court dismissed because Plaintiffs failed to allege sufficient injuries to satisfy Article III standing requirements.[29] Only one named Plaintiff, Matthew Kuhns, appealed; and the main question on appeal was whether his claimed injuries were sufficient to satisfy Article III standing.[30] Scottrade cross-appealed, claiming that even if Kuhns had standing, he had not pleaded sufficient facts for which relief could be granted.[31]

---

19. *Kuhns*, 868 F.3d at 715.

20. *Id.* at 714.

21. *Id.*

22. *Id.*

23. *Id.*

24. Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *1 (E.D. Mo. July 12, 2016), *aff'd sub nom.* Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017).

25. *Id.*

26. Those causes of action included: breach of contract, breach of implied contract, negligence, unjust enrichment, declaratory relief, and violations of multiple state statutes. *Id.* at *2.

27. Consolidated Class Action Complaint at 2, *Duqum*, 2016 WL 3683001, (No 4:11-cv-01537-SPM), 2016 WL 8459371.

28. *Duqum*, 2016 WL 3683001, at *8.

29. *Id.*

30. *Kuhns*, 868 F.3d at 715.

31. *Id.* at 714.

Kuhns argued that "Scottrade provided deficient cybersecurity in violation of its 'contractual and other obligations.'"[32] He claimed that because of that deficiency, he "faced an immediate and continuing increased risk of identity theft," incurred costs from monitoring personal accounts to mitigate risk of fraud, received diminished value of services from Scottrade, overpaid for diminished services, suffered a decline in value of his PII, and suffered an invasion of privacy.[33]

Scottrade argued that Kuhns failed to establish "'concrete facts' sufficient to plausibly suggest a certainly impending risk of future identity theft" resulting from the hack.[34] Regarding the "diminished value" claim, Scottrade argued that the fees paid were to execute stock trades – which were faithfully executed – and therefore there was no breach of contract and Kuhns received the full "benefit of the bargain."[35] Scottrade further argued that even if the Eighth Circuit were to find standing, it should dismiss the case for failure to state a claim for which relief could be granted because no actual monetary damages could be identified.[36]

The Eighth Circuit held that Kuhns had standing based on his contract claims, reasoning that customers "did not receive the full benefit of [the] bargain" and "received brokerage services of [a] lesser value" when their PII was compromised.[37] The Eighth Circuit found that Scottrade breached the contract by failing to provide "promised reasonable safeguards" contained within a privacy policy, which, in turn, caused Kuhns to suffer injury in fact sufficient to confer standing.[38] However, the court affirmed the dismissal with prejudice because Kuhns failed to plausibly allege "actual damages" in the breach of contract.[39]

B. In re SuperValu, Inc.*: Decided August 30, 2017*[40]

The second of the two cases decided by the Eighth Circuit involved the theft of customer financial information from major grocery store chains after hackers installed malicious software on point-of-sale devices in over 1,000 stores.[41] From June 22, 2014, to July 17, 2014, hackers gained access to the computer network that SuperValu used to process credit and debit card transactions.[42] The hackers installed software on that network, which allowed them

32. *Id.* at 715.
33. *Id.*
34. Defendant/Appellee/Cross-Appellant Scottrade, Inc.'s Principal and Response Brief at 31, *Kuhns*, 868 F.3d 711, (Nos. 16-3426, 16-3542), 2016 WL 6831141.
35. *Id.* at 34–35.
36. *Id.* at 14–15.
37. *Kuhns*, 868 F.3d at 716.
38. *Id.*
39. *Id.* at 714, 718.
40. 870 F.3d 763 (8th Cir. 2017).
41. *Id.* at 766.
42. *Id.*

to "harvest" customer payment information as it crossed the network.[43] This information included customer names, payment card account numbers,[44] expiration dates, card verification codes, and personal identification numbers.[45] This type of information is considered PII, and the "harvesting" of that data is considered theft.[46]

On August 14, 2014, nearly two months after the incident began, SuperValu issued a press release notifying customers of the breach and admitting that a theft of the data had potentially occurred.[47] On September 29, 2014, SuperValu announced that a second data breach had occurred after the August 2014 press release and that a different malicious software had been installed on the same network.[48] In both announcements, SuperValu acknowledged the presence of hostile software on the payment network but downplayed the notion that any data "was in fact stolen" and pledged to investigate the intrusion's scope.[49]

Sixteen customers ("Plaintiffs," collectively), representing a class who had purchased goods from SuperValu stores over a four-month period using a credit or debit card, filed four separate class actions in federal district courts in three states against three corporations that owned and operated thousands of SuperValu retail grocery stores across the country ("Defendants," collectively).[50] Defendants moved to centralize the proceedings, and the United States Judicial Panel on Multidistrict Litigation ordered the cases consolidated as a single class action in the U.S. District Court for the District of Minnesota.[51] In the amended consolidated class action complaint, Plaintiffs sought certification of the class, money damages based upon six causes of action,[52] injunctive

43. *Id.*

44. This includes data from both credit and debit cards. *Id.*

45. *Id.*

46. *Id.* at 769.

47. *Id.* at 766.

48. *Id.*

49. *Id.*

50. *In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *1–2 (D. Minn. Jan. 7, 2016), *aff'd in part, rev'd in part and remanded* 870 F.3d 763 (8th Cir. 2017). The defendants included: SuperValu Inc., a Fortune 100 corporation headquartered in Minnesota and third-largest food retailer in the United States with over 3,000 stores; AB Acquisitions, LLC, a privately held company headquartered in Idaho that owned and operated over 1,000 stores; and New Albertson's, Inc., a wholly-owned subsidiary of AB Acquisitions, LLC. Consolidated Class Action Complaint at 11–12, *In re SuperValu*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792.

51. *See In re SuperValu*, 870 F.3d at 765.

52. Those causes of action included: "(1) violations of state consumer protection statutes, (2) violations of state data breach notification statutes, (3) negligence, (4) breach of implied contract, (5) negligence per se, and (6) unjust enrichment." *Id.* at 767.

relief,[53] and attorneys' fees and costs.[54] Like *Kuhns*, the district court refused to reach the merits of the case and, upon a motion from Defendants, dismissed for lack of subject matter jurisdiction[55] for a "failure to allege facts establishing Article III standing."[56] Thus, the primary question on appeal was whether the court could find Article III standing based on a substantial and imminent risk of harm to customers who had personal data compromised by the data breach.[57]

Plaintiffs' argued that Defendants "failed to take adequate measures to protect customers' Card Information."[58] Plaintiffs first alleged that the data breach occurred because Defendants used substandard data security practices[59] that violated industry best practices and heightened the likelihood of a breach.[60] Plaintiffs additionally alleged that because numerous large data breaches had occurred targeting retailers, Defendants should have foreseen the vulnerability in their security systems and been prepared for an attack.[61] Plaintiffs claimed that because of Defendants' substandard practices and lack of foresight, they were subjected "to an imminent and real possibility of identity theft" for an "extended period of time" because of the long-term vulnerability of financial information on the digital black market.[62] One named Plaintiff, David Holmes, also claimed that a fraudulent charge appeared on his credit card shortly after Defendants' first breach announcement, and in response, he cancelled the card and waited two weeks for a replacement.[63] Defendants responded that Plaintiffs failed to allege that they suffered any actual or impending injuries, that any future injuries were "merely speculative," and that any costs incurred by Plaintiffs in protecting against a speculative injury were self-imposed harms.[64]

A unanimous three-judge panel for the Eighth Circuit affirmed the district ruling in part, reversed in part, and remanded the case to the district court for

---

53. The injunctive relief sought to enjoin Defendants from continuing the claimed "unlawful practices." Consolidated Class Action Complaint, *supra* note 50, at 40. It also asked the court to order the defendants to identify all victims and pay damages and order Defendants to begin corrective advertising campaigns. *Id.*

54. *Id.*

55. *See* FED. R. CIV. P. 12(b)(1).

56. *See In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *3 (D. Minn. Jan. 7, 2016), *aff'd in part, rev'd in part and remanded* 870 F.3d 763 (8th Cir. 2017).

57. *In re SuperValu*, 870 F.3d at 768.

58. *Id.* at 766.

59. Such as easily guessed passwords, failure to lock out users after multiple failed login attempts, and no segregation of the network by use of firewalls. *Id.*

60. *Id.*

61. *Id.*

62. *Id.* at 766–67. The specific threat was that the hackers could use the compromised data to make charges or withdrawals, open new credit accounts, or sell the data to third parties who could do the same. *Id.*

63. *Id.* at 767.

64. Brief of Defendants-Appellees at 29–32, *In re SuperValu*, 870 F.3d 763 (Nos. 16-2378, 16-2528).

further proceedings.[65] The Eighth Circuit held that there were insufficient claims in the complaint to allege "substantial risk of future identity theft" but held that only Holmes, who had claimed a present injury for the fraudulent charge on his card, had standing.[66] The court noted that a putative class action could proceed as long as *one* named Plaintiff could show standing and concluded that the district court erred in dismissing the action for lack of subject matter jurisdiction.[67] The court then affirmed the dismissal for the fifteen other Plaintiffs and remanded the case to the district court to consider the merits of the Holmes' claim.[68]

III. LEGAL BACKGROUND

Legal solutions for data breaches currently fall into two main categories – Federal Trade Commission ("FTC") enforcement actions[69] and private suits based in tort, contract, or state statute.[70] Typically, consumers bring claims involving data breaches as federal class action lawsuits,[71] as the number of potential class members is quite large and the amount of damages that each individual expects to recover is quite small.[72] Yet, to date, most data breach class action cases have been dismissed either due to a plaintiff's inability to show an injury in fact for purposes of standing or failure to state a claim for which relief can be granted.[73]

The issue of standing has led to a circuit split among the U.S. Courts of Appeal for the Sixth, Seventh, Ninth, and District of Columbia Circuits on one side and the U.S. Courts of Appeal for the Third, Fourth, and Eighth Circuits on the other.[74] The circuit split mostly concerns whether data breach victims have standing to sue an entity with the responsibility of securing PII of customers.[75] Particularly, courts have wrestled with the question of whether a data breach constitutes an injury in fact and whether a hypothetical risk of future harm (such as potential identity theft) is sufficient for standing purposes.[76] This split has yet to be resolved by the United States Supreme Court, and the

65. *In re SuperValu*, 870 F.3d at 774.

66. *Id.* at 768.

67. *Id.* at 768, 774.

68. *Id.* at 774.

69. FTC enforcement actions are outside the scope of this Note, which focuses on the Eighth Circuit decisions and the issue of Article III standing.

70. *See* David J. Baldwin, Jennifer Penberthy Buckley & D. Ryan Slaugh, *Insuring Against Privacy Claims Following a Data Breach*, 122 PA. ST. L. REV. 683, 687–706 (2018).

71. Claims are usually brought under 28 U.S.C. § 1332(d) (2018).

72. Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017).

73. *See* discussion *infra* Sections III.A, IV.A.

74. *See* discussion *infra* Section III.C.

75. *See* discussion *infra* Section III.C.

76. *See* discussion *infra* Section III.C.

Court denied a writ of certiorari based on standing in a data breach case in 2018.[77] Section A of this Part discusses the typical elements that plaintiffs in a data breach case must prove to establish Article III standing. This Section focuses on the first element of standing: injury in fact. Next, Section B highlights some legal theories plaintiffs have used to substantiate their "injury" after a data breach. Finally, Section C examines, in depth, the circuit split on standing in data breach cases.

A. Article III Standing

Standing is the major hurdle for plaintiffs to overcome when seeking legal redress for a data breach. The doctrine of standing limits the categories of litigants who can seek redress for a legal wrong within a jurisdiction to only those who have actually suffered injury.[78] For a federal case, which includes nearly all consumer suits against breached entities, standing is governed by the Cases and Controversies Clause of Article III, Section 2 of the U.S. Constitution.[79] Standing may also be created by Congress specifically by statute as long as a plaintiff can show he or she suffered concrete harm and not just a "bare procedural violation" of that statute.[80] The United States Supreme Court has interpreted standing numerous times, and the most common articulation of the doctrine came from *Lujan v. Defenders of Wildlife*,[81] which states that the "irreducible constitutional minimum" requires plaintiffs to establish that they "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of . . . defendant, and (3) that is likely to be redressed by a favorable judicial decision."[82]

In data breach cases, the first requirement of standing, injury in fact, is the most difficult for plaintiffs to establish. In fact, for a court to consider the second and third elements of standing (causality and redressability), an injury in fact must be found "[f]irst and foremost."[83] Courts rarely address the second two elements of standing because injury in fact has been so difficult for plaintiffs to prove.[84] However, when a court has found injury in fact, showing that the injury is "fairly traceable to the challenged conduct of the defendant" is relatively straightforward.[85] The final element, "redressability," has been a

77. CareFirst, Inc. v. Attias, 138 S. Ct. 981, 981 (2018) (mem.).

78. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547–48 (2016).

79. *Id.* at 1550.

80. *See id.* at 1549–50.

81. 504 U.S. 555 (1992).

82. Kuhns v. Scottrade, Inc., 868 F.3d 711, 716 (8th Cir. 2017) (quoting *Spokeo*, 136 S. Ct. at 1547).

83. *Spokeo*, 136 S. Ct. at 1547 (quoting Steel Co. v. Citizens for Better Env't, 523 U.S. 83, 103 (1998)).

84. *See* Dowty, *supra* note 72, at 695.

85. *See id.* at 694.

challenge for plaintiffs in a handful of cases because the nature of the harm is often abstract.[86]

To prove an injury in fact, the United States Supreme Court has stated that plaintiffs must show "'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[87] In data breach cases, both the "concrete and particularized" and the "actual or imminent" requirements have been difficult to overcome because most plaintiffs cannot show that the breach of their PII caused any tangible harm.[88]

1. "Concrete and Particularized"

An injury is "particularized" when it "affect[s] the plaintiff in a personal and individual way."[89] In terms of a data breach, each plaintiff's "personal interests" in the mishandling of their PII is "individualized rather than collective."[90] However, particularization alone does not establish an injury in fact; rather, the "concreteness" of an injury must also be established.[91] For an injury to be "concrete," it must "actually exist," meaning it must be "real[] and not abstract."[92] This does not necessarily mean that the injury must be "tangible," as intangible harms can constitute a real harm.[93] The United States Supreme Court has recently noted that a "risk of real harm," which is clearly intangible, can satisfy the concreteness element.[94] For a data breach, in which the primary risk of harm is identity theft, "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury."[95]

86. *See id.* at 695.

87. *Spokeo*, 136 S. Ct. at 1548 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

88. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010).

89. *Spokeo*, 136 S. Ct. at 1548 (quoting *Lujan*, 504 U.S. at 560).

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.* at 1549.

94. *Id.*; *see also* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–55 (2010) (stating that a "substantial risk" of cross-contamination of crops was sufficient injury to find standing).

95. Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) (mem.).

2. "Actual or Imminent"

The United States Supreme Court recently examined the requirement of imminence in *Clapper v. Amnesty International USA*.[96] Without reaching the merits of plaintiff's argument, the Court held that Article III standing was unavailable for a lack of imminence.[97] The Court admitted that a threat of a "future injury" could be enough to confer Article III standing but only if it is "certainly impending."[98] However, if the future injury is "speculative" and based on a "highly attenuated chain of possibilities," then it cannot be characterized as "imminent."[99] Finding standing in data breach cases has become a more challenging hurdle since *Clapper* because the risk of harm from a data breach is often based only on potential identity thefts – an event that has not yet occurred and may not ever occur.

B. Legal Theories on Which Plaintiffs Have Relied

Consumers affected by a data breach attempted to use many theories in courts to seek remedy for the "harm" of PII exposure. In the past few years alone, plaintiffs have brought suits for "negligence, breach of contract, unjust enrichment, breach of fiduciary duty, unfair and deceptive business practices, invasion of privacy," and violations of various state and federal statutes.[100] Even when plaintiffs in data breach cases successfully establish standing, few claims have resulted in successful relief under common law principles.[101] Courts have been rather consistent in finding that the mere risk of future harm from a data security breach does not rise to the level of compensable harm.[102]

---

96. 568 U.S. 398 (2013).

97. *Id.* at 422. In *Clapper*, plaintiffs were a group of non-profit, legal, and media organizations who argued that § 702 of the Foreign Intelligence Surveillance Act was unconstitutional because it allowed the government wide berth to eavesdrop on their communications with overseas contacts. *Id.* at 401, 406. Plaintiffs claimed that there was an "objectively reasonable likelihood" that their communications would be intercepted "at some point in the future" and that they would have to travel overseas or cease communicating with those contacts to circumvent the potential surveillance. *Id.* at 401, 407.

98. *Id.* at 409.

99. *Id.* at 410.

100. Dowty, *supra* note 72, at 686; *see also, e.g.*, Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012); *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017); *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953 (N.D. Cal. 2016); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. 2014).

101. *See* Elizabeth T. Isaacs, Comment, *Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*, 67 OKLA. L. REV. 519, 522 (2015).

102. *See* Jay M. Zitter, Annotation, *Liability for Risk of Future Identity Theft*, 50 A.L.R. 6th 33, § 6, West (database updated weekly).

Even if damages could be proven, problems exist with proving causation. Plaintiffs must show that identity theft or other ill-begotten use of PII was caused by the data breach in question and not by some prior breach or lawful dissemination of the data.[103]

C. The Circuit Split

The U.S. Courts of Appeal for the Sixth, Seventh, Ninth, and District of Columbia Circuits have consistently been the most likely to find standing in data breach cases. These circuits have allowed victims of a data breach to sue when PII is merely exposed to hackers and there is not yet evidence of fraudulent credit card charges[104] or the hackers' understanding of the data they breached.[105] The Third, Fourth, and (now) Eighth Circuits have applied more scrutiny to plaintiffs seeking standing in data breach cases. In these circuits, plaintiffs must do more than merely allege that PII was exposed to hackers. These circuits have required evidence that the breached data was *actually* used to the detriment of the victims or that the breaching party understood the value of the data and had actual plans to misuse it.

1. Circuits More Likely to Find Standing: Sixth, Seventh, Ninth, and District of Columbia

The Sixth, Seventh, Ninth and District of Columbia Circuits have interpreted standing requirements for plaintiffs affected by a data breach more liberally. First, each circuit has found that PII exposed in a data breach signifies some future risk of "concrete" harm of identity theft. Second, each circuit has found that costs incurred by consumers seeking to mitigate that future harm is not self-inflicted and constitutes either an injury in fact or some measure of redressable damages. Finally, each circuit has found that the imminence issue from *Clapper* does not pose a substantial barrier to the claims of future harm.

The Sixth Circuit recently found standing for customers of an insurance company that had over 1.1 million records containing PII compromised.[106] The Sixth Circuit analyzed the risk of the future harm standard laid out in *Clapper* and determined that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes . . . ."[107] The court further stated that there was "no need for speculation" when data had been allegedly stolen and was "in the

103. *See* Isaacs, *supra* note 101, at 543–44.

104. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966–69 (7th Cir. 2016).

105. *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014).

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

107. *Id.* at 388.

hands of ill-intentioned criminals."[108] Rejecting the argument that credit monitoring costs were "self-inflicted" in anticipation of non-imminent harm, the court reasoned that the continuing risk of identity theft and the tangible costs of monitoring financial accounts for unauthorized activity constituted a harm.[109] The court placed an emphasis on the fact that the insurance company explicitly suggested that consumers affected by the breach actively monitor their accounts, which seemed to contravene the company's argument that the harm was not "concrete."[110]

The Seventh Circuit recently reaffirmed its liberal theory of standing for consumers affected by a credit card data breach in *Lewert v. P.F. Chang's China Bistro, Inc*.[111] Two plaintiffs brought suit, one claiming fraudulent charges had appeared on a debit card shortly after eating at a P.F. Chang's restaurant and the other claiming he suffered harm by spending time monitoring his credit report and card statements after the announcement of the breach, although he did not suffer any fraudulent charges.[112] The court found both plaintiffs had standing.[113] The court determined that it was "plausible to infer a substantial risk of harm from the data breach[] because a primary incentive for hackers is 'sooner or later[ ] to make fraudulent charges or assume those consumers' identities.'"[114] Regarding the immediacy requirement, the court observed that because the breach had already occurred, the risk of identity theft and fraudulent charges was "sufficiently immediate to justify mitigation efforts."[115] The court concluded that "time and money spent resolving fraudulent charges [were] cognizable injuries for Article III standing."[116]

In *Krottner v. Starbucks Corp.*, the Ninth Circuit found standing for 97,000 Starbucks employees whose unencrypted names, addresses, and social security numbers were stored on a stolen laptop computer.[117] Starbucks sent notice to the affected employees and offered free credit monitoring services.[118] Despite the fact that none of the employees suffered any financial loss, the Ninth Circuit held that they suffered an injury in fact because they experienced "a credible threat of harm" that was "both real and immediate."[119] The court held "that [individuals] whose personal information [had] been stolen but not

108. *Id.*
109. *Id.* at 388–89.
110. *See id.* at 389.
111. 819 F.3d 963, 965 (7th Cir. 2016).
112. *Id.*
113. *Id.* at 970.
114. *Id.* at 967 (alteration in original) (quoting Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).
115. *Id.*
116. *Id.* at 967.
117. 628 F.3d 1139, 1140 (9th Cir. 2010).
118. *Id.* at 1140–41.
119. *Id.* at 1143.

misused[] [had] suffered an injury sufficient to confer standing . . . ."[120] Although the *Krottner* case was decided before *Clapper*'s apparent narrowing of the imminence requirement in 2013, the U.S. District Court for the Southern District of California later adhered to *Krottner*'s reasoning when it found that an injury in fact occurred simply because hackers breached a system containing PII and could have accessed the information in *In re Sony Gaming Networks* in 2014.[121]

In *Attias v. CareFirst, Inc.*, the District of Columbia Circuit held that approximately one million customers of a health insurance company whose PII was subjected to a breach had plausibly alleged a substantial enough risk of future injury to create Article III standing.[122] The court stated that "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm . . . 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."[123] Agreeing with plaintiffs that identity theft constituted a "concrete and particularized injury" and that the nature of the information breached could plausibly create a "substantial risk of identity fraud," the court found that plaintiffs satisfied *Clapper*'s imminence test.[124] Finally, the court addressed redressability by considering the costs incurred by plaintiffs to "mitigate or avoid [the] harm" of identity theft and found that any money spent could be reimbursed to make plaintiffs whole.[125]

2. Circuits Less Likely to Grant Relief: Third, Fourth, and Eighth

The Third, Fourth, and Eighth Circuits have been more resistant in finding standing for plaintiffs in a data breach case. The Third and Fourth Circuits, in particular, have placed significant roadblocks in front of plaintiffs by rejecting allegations of "hypothetical, future injur[ies]" and finding plaintiffs' concerns

120. *Id.* at 1140.

121. *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014); *see also In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214–15 (N.D. Cal. 2014) (finding standing when hackers accessed credit card information despite no allegations of misuse). *But see In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–59 (D. Nev. 2015) (holding that the immanency requirement was not met because there was no evidence of misuse three years after the breach and the passage of time showed no "substantial risk" of harm).

122. 865 F.3d 620, 622–23, 626 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) (mem.).

123. *Id.* at 627 (quoting Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 915 (D.C. Cir. 2015)).

124. *Id.* at 628–29.

125. *Id.* at 629.

about potential identity theft to not be "imminent" enough to warrant standing.[126] As described *infra*, the Eighth Circuit has found standing in limited circumstances but has rejected plaintiff claims of compensable harm.[127]

The leading case in the Third Circuit as of the time this Note was written is *Reilly v. Ceridian Corp.*[128] In *Reilly*, a payment processor that collected employees PII to issue paychecks for over 1,900 companies suffered a security breach, but it was unclear if the hacker "read, copied, or understood the data."[129] The court held that the allegations of "hypothetical, future injury" were insufficient to confer standing.[130] Noting that it was pure speculation to determine if the hacker actually was aware of the data it accessed, if the hacker intended to commit any future criminal acts with the information, and if the information itself could be used to the detriment of plaintiffs, the court rejected any claim of harm.[131] The court further dismissed the notion that "incurred expenses in anticipation of future harm," such as spending time, effort, and money on credit monitoring, were sufficient to confer standing.[132] The court did not completely close the door to future suits and suggested, in dicta, that if it could be shown that breached information "[was] actually read, copied, understood, and misused to a plaintiff's detriment," standing would be available.[133]

The Fourth Circuit likely has the least plaintiff-friendly interpretation of the standing doctrine in data breach cases, as shown in its comprehensive denial of standing in *Beck v. McDonald*.[134] In *Beck*, a laptop from a veteran's hospital containing unencrypted PII of 7,400 patients went missing and was considered stolen.[135] Plaintiffs, Veterans Affairs ("VA") patients, brought claims against the Secretary of VA, alleging federal statutory violations[136] and an increased risk of harm for future identity theft.[137] Plaintiffs also claimed mitigation costs because they had to "frequently monitor their credit reports, bank statements, health insurance reports, and other similar information, purchas[e] credit watch services, and [shift] financial accounts."[138]

The Fourth Circuit disagreed with both claims and distinguished the decisions from the Sixth, Seventh, and Ninth Circuits that had found standing

126. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 41, 46 (3d Cir. 2011).
127. *See infra* Part IV.
128. 664 F.3d at 38.
129. *Id.* at 40.
130. *Id.* at 42.
131. *Id.*
132. *Id.* at 46.
133. *Id.* at 45.
134. *See* 848 F.3d 262 (4th Cir.), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017) (mem.).
135. *Id.* at 267.
136. Plaintiffs alleged violations of the Privacy Act of 1974 and the Administrative Procedure Act. *Id.* at 266.
137. *Id.* at 266–67.
138. *Id.* at 267 (alteration in original) (internal quotations omitted).

after a data breach based on factual differences.[139] Analyzing the "imminence" prong in light of *Clapper*, the *Beck* court found plaintiffs' claims too speculative and attenuated because, in the three years that had passed since the laptop was stolen, plaintiffs were unable to produce evidence showing that their PII had been accessed or misused or that they had suffered from identity theft.[140] To find harm of future identity theft, the court said it would have to construct an "attenuated chain of possibilities," which the *Clapper* court expressly rejected.[141] Then, regarding "substantial risk" of future harm, the court rejected an argument by plaintiffs that thirty-three percent of data breaches result in victims of identity theft by pointing out that the number was just a "general statistic" that had little bearing on the unique facts of the case at hand.[142] Further, unlike the other circuits, the court "decline[d] to infer a substantial risk of harm of future identity theft" because of the VA's offer to provide credit monitoring services.[143] The court reasoned that making such a ruling may discourage companies subject to a future breach from offering to provide such credit monitoring services.[144] Finally, the court rejected the mitigation costs argument by stating that "self-imposed harms cannot confer standing."[145]

IV. INSTANT DECISIONS

The two separate Eighth Circuit panels in *Kuhns* and *In re SuperValu* each found limited standing for Plaintiffs but for completely different reasons. Additionally, each panel chose a different path when determining redressability for Plaintiffs. This Part will first examine the outcome in *Kuhns*; next, it will examine *In re SuperValu*.

A. Kuhns v. Scottrade, Inc.

Citing Eighth Circuit precedent,[146] the court concluded that Kuhns had standing for his contract-related claims because "he did not receive the full benefit of his bargain with Scottrade."[147] The court affirmed that "a party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged."[148] Because a portion of the fees

139. *Id.* at 273, 276.

140. *Id.* at 274–75.

141. *Id.* at 275 (quoting Clapper v. Amnesty Int'l USA, 588 U.S. 398, 410 (2013)).

142. *Id.* at 275–76, 276 n.7.

143. *Id*. at 276.

144. *Id.*

145. *Id.* at 276–77.

146. Carlsen v. GameStop, Inc., 833 F.3d 903, 909 (8th Cir. 2016) (finding that a company's privacy policy contained within terms of service created a contractual relationship that was breached when the company shared confidential personal information with third parties).

147. Kuhns v. Scottrade, Inc., 868 F.3d 711, 716 (8th Cir. 2017).

148. *Id.* (quoting *Carlsen*, 833 F.3d at 909).

for brokerage services were used to meet Scottrade's "contractual obligations to provide data management and security," the breach of those obligations meant those services were diminished in value.[149] The court held that this was enough of a "concrete and particularized" allegation of breach of contract to confer "actual" injury.[150]

The Eighth Circuit reviewed the district court's decision in *Kuhns* de novo because Scottrade made a successful summary judgment motion on standing.[151] Kuhns alleged that standing existed because he faced "an immediate and continuing increased risk of identity theft;" incurred mitigation costs; "received Brokerage Agreement services diminished in value" and therefore did not receive the full benefit of the bargain; suffered harm from the decline in value of PII; and suffered an invasion of privacy.[152] In determining standing, the court – somewhat paradoxically – ignored all the claims but the benefit of the bargain claim.[153]

The next question addressed by the court was whether to dismiss the case for failure to state a claim for which relief could be granted.[154] The court analyzed each of Kuhn's four claims for relief individually but ultimately rejected all of them.[155] First, the court considered a claim for breach of express contract.[156] Noting that the complaint neither identified any actual misrepresentations nor "applicable [data security] law and regulation" breached by Scottrade, the court concluded that Kuhns' "bare assertions" of a failure to protect customer PII were not plausible enough to allege "actual damage."[157] The court also observed that the express terms of the contract did not appear to contemplate data management or security.[158] The court concluded that because no fraud or identity theft had resulted from stolen PII in the two years since the breach was identified, it was inappropriate to base massive class action litigation on mere "allegations of worry and inconvenience."[159]

Second, the court dismissed Kuhn's claim of implied breach of contract for a failure to allege a plausible claim.[160] Despite the brokerage agreement

149. *Id.*

150. *Id.*

151. *Id.* at 715. The court noted that Kuhns had filed to voluntarily dismiss the case after fully briefing the court and prior to oral arguments because of another action on the matter that was proceeding in California state court; however, the court considered the motion untimely and proceeded. *Id.* at 715, 719.

152. *Id.* at 715.

153. *See id.* at 716.

154. *Id.*

155. *Id.* at 717–19. The four claims were: (1) breach of express contract; (2) breach of implied contract and unjust enrichment; (3) declaratory relief; and (4) breach of the MMPA, a consumer protection statute. *Id.*

156. *Id.* at 717–18.

157. *Id.* (citing Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)).

158. *Id.* at 718.

159. *Id.*

160. *Id.*

containing language that the company utilized "industry leading" security measures, the court declined to speculate about whether it implied an additional contract term because of a lack of any cognizable industry standard.[161] Third, the court dismissed Kuhn's claim for declaratory relief that Scottrade "stop its illegal practices" because it concluded the claim was "virtually unintelligible" and only "focuse[d] on past conduct . . . not on Scottrade's current practices."[162] Finally, the court dismissed Kuhn's fraud claim under the Missouri Merchandising Practices Act ("MMPA") because it found that the statute only covered fraud in relation to the "sale of merchandise."[163] Noting that intangible services can qualify as merchandise, the court further determined that Scottrade was selling brokerage services, not data security services, and that any customers' transfer of PII was "voluntarily transfer[ed]" to obtain access to those brokerage services.[164]

B. In re SuperValu, Inc.

This case was also reviewed de novo by the Eighth Circuit.[165] The main question for the court in *In re SuperValu* was whether Plaintiffs had adequately alleged a "'certainly impending' or 'substantial risk' of identity theft as a result of the data breaches."[166] The court began by dismissing standing-based arguments from the Sixth, Seventh, and District of Columbia Circuits by claiming that the facts were distinguishable.[167] It then agreed that the facts supported a conclusion that the hackers actually stole credit card information from Plaintiffs and had not merely gained access to the data.[168] The court then observed that only Holmes alleged any fraudulent transactions on a financial account and that the other Plaintiffs' allegations rested "on information and belief [that] illicit websites [were] selling their Card Information to counterfeiters and fraudsters."[169] The court considered these allegations to be too speculative rather than "certainly impending" and concluded that Plaintiffs failed to show any injury.[170]

---

161. *Id.*
162. *Id.*
163. *Id.* at 718–19.
164. *Id.* at 719.
165. *In re* SuperValu, Inc., 870 F.3d 763, 768 (8th Cir. 2017).
166. *Id.* at 769.
167. *See id.* The court did not elaborate on the factual differences between the cases in sister circuits and the case at hand. *See id.* However, the cases cited by the court here included instances in which PII was compromised from two separate insurance databases, a healthcare database, and malware installed on two separate point-of-sale systems. *See id.*
168. *Id.*
169. *Id.* at 769–70.
170. *Id.*

After concluding that identity theft "constitutes an actual, concrete, and particularized injury," the court next determined whether the mere risk of future identity theft could be considered "substantial."[171] The court examined the nature of the data stolen: credit card information.[172] Credit card information typically does not accompany any sensitive PII and "generally cannot be used alone to open unauthorized new accounts."[173] Concluding that there was "little to no risk" that fraudulent accounts could be opened in the name of Plaintiffs, the court held that the mere theft of the information did not create a substantial enough risk to constitute injury in fact.[174] The court then went a step further and addressed the mitigation costs borne by Plaintiffs, holding that "[b]ecause [P]laintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury."[175] Thus, standing was denied for all Plaintiffs who merely alleged a future risk of harm.[176]

For Holmes – the named Plaintiff who alleged present injury – however, the court was more lenient. Stating that "the misuse of Holmes' Card Information is credit card fraud and thus a form of identity theft," the court answered whether the complaint had alleged sufficient causation to link the breach to the fraud in the affirmative.[177] Defendants argued that the present harm theory should be dismissed because it had not been argued in the complaint.[178] However, the court noted that "it is unnecessary to set out a legal theory for . . . [P]laintiff's claim for relief in a pleading" so long as the alleged facts demonstrate actual injury.[179] The court then analyzed four elements to determine potential causation: (1) Defendants failed to secure the data on their network, (2) the network was subsequently hacked, (3) the data was stolen by hackers, and (4) Holmes became a victim of identity theft after the breaches.[180] The court stated that Holmes met his "modest" burden of alleging that the fraudulent charge was "fairly traceable" to Defendants' breach.[181]

Defendants next argued that even if Holmes had alleged standing for a present injury, his allegation was insufficient to provide standing for the rest of

---

171. *Id.* at 770.

172. *Id.* at 770–71.

173. *Id.* at 770 (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 30 (2007)). To be classified as PII, the data would have to be similar to "social security numbers, birth dates, and driver's license numbers." *See id.*

174. *Id.*

175. *Id.* at 771.

176. *Id.* at 771–72.

177. *Id.* at 772–73.

178. *Id.* at 772.

179. *Id.* (quoting Johnson v. City of Shelby, 135 S. Ct. 346, 347 (2014)).

180. *Id.*

181. *Id.*

the class, who had only alleged risk of future harm without evidence of "widespread misuse."[182] The court held that each class member's standing must be "assessed individually" and that it was error to make Holmes' standing dependent on the standing of other named and unnamed Plaintiffs.[183] The court stated, "To the extent Holmes can show that the fraudulent charge was unreimbursed, such financial harm would be compensable in this action."[184] Thus, this panel of the Eighth Circuit forged its own path in the circuit split by finding standing for a present injury while rejecting any claim for potential future injury even though Plaintiffs had incurred mitigation costs in response to the breach.[185]

V. COMMENT

This Part proceeds in three Sections. Section A discusses the contributions of *Kuhns* and *In re SuperValu* to current law in data breach cases. Section B discusses what plaintiffs filing a case in the Eighth Circuit should consider before bringing a data breach case. Finally, Section C concludes with thoughts on expected changes in the law regarding data breach litigation.

A. The State of the Law After Kuhns *and* In re SuperValu

The Eighth Circuit's contribution to the panoply of law surrounding data breaches is further proof that the United States Supreme Court needs to revisit its voluminous Article III standing jurisprudence and articulate a new doctrine for the digital age. The series of decisions since *Lujan* have only further obscured the meaning of injury in fact. The divergent course of the circuits provides clear evidence of this confusion. For instance, some circuits have no problem finding harm from mitigation costs borne by plaintiffs when a data breach occurs, while others consider such costs to be a self-imposed harm.[186] Some circuits agree that the risk of future harm from compromised PII is sufficient to find standing, while others believe it is too speculative.[187]

The Eighth Circuit's decisions are curious because the court found standing but ultimately rejected both mitigation costs and risk of future harm as injuries.[188] Therefore, it effectively shut the door on any recovery for plaintiffs unless they can prove actual identity theft. Tracing identity theft to a particular breach is a problem in itself, particularly as more and more sources containing sensitive PII are breached. Restricting plaintiff recovery to actual, traceable

182. *Id.* at 772–73. The district court had accepted this argument in its opinion for dismissal. *Id.* at 773.

183. *Id.* at 773.

184. *Id.*

185. *See id.* at 774.

186. *See supra* Section III.C.

187. *See supra* Section III.C.

188. *See supra* Part IV.

identity theft may make it nearly impossible for Eighth Circuit plaintiffs to obtain standing if their data is subject to breach. This will likely reduce the number of cases brought in the Eighth Circuit, as putative plaintiffs will likely seek the more favorable jurisdictions of the Sixth and Seventh Circuits.

The *Kuhns* decision is particularly vexing. The court found standing on a contract theory but then rejected any compensable harm for breach of that contract.[189] Nearly every online service contains some sort of privacy policy that could be interpreted as forming an implied contract. If any payment is made for those services, then customers whose data is breached lose the "benefit of the bargain" in the form of diminished value for those services. By dismissing Kuhns' claims for failure to state a claim for which relief could be granted pursuant to Federal Rule of Civil Procedure 12(b)(6), the bar set for plaintiffs was raised even higher.

After *Kuhns*, plaintiffs who paid a service fee with an associated privacy policy will likely be found to have standing in the event of a breach but will still be ineligible for any recovery based on any risk of future harm. Parties that have been subject to a data breach need only to take steps to mitigate future harm, such as notifying its customers or providing credit monitoring services, to reduce their potential liability. These mitigation steps may keep the problem from worsening, but these steps do not put customers in the same position that they were before the breach occurred, and the breach of contract would go without remedy.

The United States Supreme Court denied writ of certiorari in *Attias v. CareFirst, Inc.*,[190] leaving the decisions in both *Kuhns* and *In re SuperValu* as the most recent statement on data breach jurisprudence in the Eighth Circuit as of the time this Note was written. The two decisions tilt the weight of the majority of circuits in favor of finding no compensable relief for risk of future harm when a breach occurs.[191] Most circuits seem content to follow their own precedents at the moment.[192] Until the Court grants a writ of certiorari in a data breach case, Congress takes action to address the issue, or the FTC engages in significant rulemaking, few major changes can be expected in data breach jurisprudence.

B. Considerations When Bringing Data Breach Suits in the Eighth Circuit

Lawyers representing plaintiffs who seek standing and recovery for a data breach action should make sure to follow a few basic principles. First, they should make sure that plaintiffs have a credible allegation of identity theft that is somehow traceable to the data breach. The record is littered with dismissed

189. *See supra* Section IV.A.
190. 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018) (mem.).
191. *See supra* Section III.C.
192. *See supra* Section III.C.

cases because plaintiffs could only claim some speculative future harm.[193] Allegations of identity theft not only are important for finding standing but are also likely needed for any chance of damage recovery.[194] The decisions in *Kuhns* and *In re SuperValu* have shown that the mere risk of identity theft is not enough.

Second, other forms of relief may be available – i.e., prospective relief, such as credit monitoring or an injunction mandating security improvements.[195] A settlement that includes injunctive relief may have greater value than a settlement granting relief in the form of identity theft damages alone.[196] Third, it is important to consider other parties that may have some share in the liability, such as third-party vendors.[197] If another party has a share of the responsibility for the breach, it may increase the pressure on defendants to reach a settlement, as one party would no longer bear the brunt of any damages.[198] Finally, attorneys should consider both common law and statutory claims, as many states have created a private cause of action for litigants in the event of a breach of PII.[199] While the odds are stacked against recovery of actual pecuniary damages for plaintiffs in the Eighth Circuit, some courts have been willing to grant some varieties of relief,[200] and settlement options may make it worth an attorney's time.

C. Inching Towards a Solution

As long as the bulk of consumer claims against breached entities fail, little incentive exists for institutional changes in data management policies to be made. Parties holding PII may be aware that improper stewardship of data may bring about FTC enforcement, but limited agency resources can only focus on the most egregious violators.[201] Yet, as the risks of data breaches become more

193. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 271–72 (4th Cir.), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017) (mem.); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

194. *See* Aaron Blumenthal & Andre M. Mura, *In the Breach*, TRIAL, Sept. 2017, at 30, 31–32.

195. *Id.* at 32.

196. For instance, settlements with Adobe and Target after a data breach derived nearly all value from injunctive mandates, such as regular auditing, system monitoring, and employee security training. *Id.* at 32. For attorneys litigating a case, this value becomes calculated in the eventual costs billed to the losing party.

197. *Id.* at 32–33.

198. *Id.* at 33.

199. At least thirteen states have passed legislation requiring certain standards for how private data stewards can manage to collect data about residents. For a list of these statutes, see *Data Security Laws: Private Sector*, NAT'L CONFERENCE OF STATE LEGISLATURES (Oct. 15, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

200. *See* Blumenthal & Mura, *supra* note 194, at 32–33.

201. *See* Baldwin, Buckley, & Slaugh, *supra* note 70, at 703–05.

public, and when a major settlement or judgment is rendered against a data steward, there will likely be a rapid shift towards self-regulation within the industry.

Holders of PII will need a clear understanding of exactly what is being collected, how it is being stored, and what security measures are being employed. Data minimization strategies[202] will be more likely employed, and PII that may induce monetary liability might be encrypted or deleted in order to avoid potential liability. Emerging technologies, such as encrypted signatures, may have to replace a social security number, date-of-birth, mother's maiden name, and driver's license number as a means of verification. Also, because of decisions like *Kuhns*, privacy policies and promises made to consumers will likely be changed to avoid giving plaintiffs a potential cause of action.

Some commenters have argued for the creation of a negligence cause of action called the "negligent enablement of cybercrime," which could be directed at entities who produce "defective products and services that pave the way for third party cybercriminals who exploit known vulnerabilities."[203] This new cause of action would create "a modified duty of care on the part of software licensors to incorporate reasonable security into their products and services."[204] These commentators suggest the new tort would likely need to be created by statute and would need to be based on existing principles of warranties, premises liability, and negligence-based products liability from the Uniform Commercial Code.[205] The development of a new standard would not be easy, but there are examples of successful implementation of similar standards in the Payment Card Industry ("PCI").[206] Lessons could be drawn from this relatively recent, successful implementation of a new standard that was implemented by industry actors instead of by government fiat.[207] It is clear, however, that the existing causes of action are insufficient for granting relief to those harmed by a data breach.

---

202. Data minimization is the process of removing or destroying unnecessary data from vulnerable locations. Sona R. Makker, *Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things*, 85 UMKC L. REV. 895, 903 (2017).

203. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1553 (2005).

204. *Id.* at 1557.

205. *Id.* at 1558, 1594. Premises liability is built on the idea that those who are aware of dangerous conditions upon their premises and take no immediate steps to fix the conditions are liable for the consequences. *Id.* at 1581–82. In terms of software, this would mean failure to patch known vulnerabilities in defective code. *Id.* at 1582.

206. The standard is called Payment Card Industry Data Security Standard ("PCI DDS") and was "developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally." John A. Fisher, Note, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 226 (2013).

207. For instance, the development of the PCI standards came through a collaborative effort between the major payment card companies and is governed by representatives from each participating member. *See About Us*, PCI SEC. STANDARDS COUNCIL,

The issue has remained at the forefront of the national conversation. In November 2018, Senator Ron Wyden of Oregon announced draft legislation that would "empower consumers to control their personal information, create radical transparency into how corporations use and share their data, and impose harsh fines and prison terms for executives at corporations that misuse Americans' data."[208] The bill, titled the "Consumer Data Protection Act,"[209] proposed to strengthen the authority of the FTC, giving it broad new powers to be "an effective cop on the beat."[210] The draft language would empower the FTC to establish minimum privacy and cybersecurity standards, issue steep fines and criminal penalties when those standards are broken, create a national "Do Not Track" system that allows consumers to restrict what third party companies can do with PII, give consumers a system to review which companies have their PII and how it is used, and require companies that have consumer PII to review how that data is managed.[211]

Senator Wyden's draft bill is ambitious, but it stands little chance of becoming law as it is written. Current political headwinds blow against an expansion of the administrative state. Not to mention the scope of the proposed sanctions for certain data breaches is troubling.[212] Also, it would take many years for the FTC to build out its enforcement mechanisms, during which time the provisions of the bill would likely be under constant challenge in federal court. The case law surrounding data breaches makes it clear that the judiciary will not be arriving at a unified solution unless the United States Supreme Court finally grants certiorari in a data breach case. Senator Wyden's bill (and other federal bills like it)[213] are necessary parts of the puzzle. A proposed legislative fix stakes out the parameters of the problem and signals to both companies that hold consumer PII and to the public at large that the status quo is untenable.

---

https://www.pcisecuritystandards.org/about_us/ (last visited Mar. 9, 2019). While the number of entities that control or manage potentially sensitive consumer PII is far larger than the limited number of payment card processors, the PCI model shows that collaborative efforts among stakeholders can be effective at creating a self-regulatory environment.

208. Press Release, Ron Wyden, Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy (Nov. 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

209. S. 2188, 115th Cong. (2017).

210. Wyden, *supra* note 208.

211. *Id.*

212. For instance, the bill considers the imposition of penalties of up to four percent of annual revenue for a company who breaches the standards on the first offense alone. *Id.* The law would also sanction criminal penalties for senior executives of up to twenty years. *Id.*

213. Data privacy bills are regularly introduced in both Houses of Congress, but they rarely (if ever) escape from the committee process. *See, e.g.*, American Data Dissemination Act of 2019, S. 142, 116th Cong. §1 (2019); Data Care Act of 2018, S. 3744, 115th Cong. §2 (2018); Cyber Privacy Fortification Act of 2015, H.R. 104, 114th Cong. §1 (2015).

The failure of Congress to pass any of the comprehensive data privacy bills proposed in the past few years does not bode well for Senator Wyden's current iteration, but with each subsequent mass data breach, the pressure for Congress to act rises.

A better solution would take a page from the promulgation of the PCI standards. Industry leaders should work together to establish what the standards for security of consumer PII should be in each sector. Instead of relying on the FTC to create a new standard out of whole cloth, as proposed in the Wyden bill, Congress should work with stakeholders to develop standards for the collection and management of consumer PII so that enforcement is not so reliant on FTC action. A statute that clearly spells out when the victim of a data breach has standing to pursue a private right of action would give the FTC some improved tools for enforcement against entities that refuse to adhere to the industry defined standards, set commonsense penalties for those who negligently allow data breaches to occur, and acknowledge that the difficulties of complete data protection would be a more complete effort. Relying solely upon the courts to solve the mess caused by the thousands of data breaches that occur each year will not yield a workable solution for quite some time.

VI. CONCLUSION

The current state of the law regarding data breaches is, quite frankly, all over the place – as evidenced by the enormous volume of cases concerning the matter. Organizations that suffer a breach may be liable to the FTC, state governments, and consumers in private actions.[214] This uncertainty is enormously inefficient and frustrating for plaintiffs' attorneys who may wish to pursue a case. Consumers have used a scattershot of legal actions to seek redress and have largely come up empty.[215] The results in *Kuhns* and *In re SuperValu* provide further examples of this chaos.[216] Few changes to the legal framework appear to be on the horizon unless Congress takes action, the FTC engages in significant regulatory rulemaking, or the United States Supreme Court agrees to take a case on the matter. The value of a person's PII diminishes each time a major breach occurs, and eventually, the market may simply have to develop better methods of verifying identity. Privacy of PII, at least as it has come to be understood, appears to have become a casualty of the digital age; and the truth is, if private information is put online, someone will try to steal it.

214. *See supra* Part III.
215. *See supra* Section III.B.
216. *See supra* Part IV.