# LIFE IS SHORT. GO TO COURT: ESTABLISHING ARTICLE III STANDING IN DATA BREACH CASES

MEGAN DOWTY*

TABLE OF CONTENTS



* Senior Editor, Southern California Law Review, Volume 90. J.D. Candidate, University of Southern California Gould School of Law (2017); B.A. Political Science and Minor in Public Affairs, University of California, Los Angeles (2014). Thank you to my parents, Phil and Susan Dowty, for all of their love and support and making me who I am today. Thank you to Professor Altman for his guidance, feedback, and mentorship during the note-writing process.

## INTRODUCTION

This is the digital age. As "the ratings machine, DJT [Donald J. Trump],"[1] says, "all I know is what's on the internet,"[2] or "the cyber," as

1. This is a term that the 45th President of the United States, Donald J. Trump, has used to refer to himself. @realDonaldTrump, TWITTER (Jan. 6, 2017, 4:34 AM), https://twitter.com/realDonaldTrump/status/817348644647108609?ref_src=twsrc%5Etfw.

2. Steve Benen, *Donald 'All I Know Is What's On The Internet' Trump*, MSNBC: MADDOW

he calls it.[3] People's use of and dependency on the Internet has made data breaches a serious and widespread threat to people's privacy and security. In 2016, there were 1,093 data breaches, up from 780 in 2015.[4] 75.6% of companies suffered at least one successful attack.[5] Essentially "there 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]

Major companies such as LinkedIn, Target, Ebay, Yahoo, Anthem, and Ashley Madison have been subject to data breaches,[7] and subsequently to lawsuits.[8] Not only can data breaches threaten people's financial security, but breaches like Ashley Madison's—a dating site whose slogan up until July 2016 was "Life is Short. Have an Affair"[9]—can threaten people's home lives and shatter careers.[10] The government is not immune to dangerous cyber attacks either. Both the U.S. Office of Personnel Management and the Democratic National Committee ("DNC") have suffered breaches.[11] Presidential candidate Hillary Clinton's e-mails were leaked as part of the DNC breach, which became a source of controversy

BLOG (May 4, 2016), http://www.msnbc.com/rachel-maddow-show/donald-all-i-know-whats-the-internet-trump.

3. Adrienne LaFrance, *Trump's Incoherent Ideas About 'the Cyber*,*'* ATLANTIC (Sept. 27, 2016), https://www.theatlantic.com/technology/archive/2016/09/trumps-incoherent-ideas-about-the-cyber/501839/.

4. IDENTITY THEFT RES. CTR., DATA BREACH REPORTS: 2016 END OF YEAR REPORT 4 (Jan. 18, 2017) [hereinafter 2016 DATA BREACH REPORTS], http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf; IDENTITY THEFT RES. CTR., DATA BREACH REPORTS: DECEMBER 29, 2015, AT 4 (Dec. 29, 2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

5. 2016 DATA BREACH REPORTS, *supra* note 4, at 7.

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 (Apr. 22, 2013), https://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/).

7. *World's Biggest Data Breaches*, INFORMATIONISBEAUTIFUL (Jan. 5, 2017), http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

8. *See, e.g.*, *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594 (N.D. Cal. May 27, 2016*)*; *In re* LinkedIn User Privacy Litig., 309 F.R.D. 573 (N.D. Cal. 2015).

9. Nathan Bomey, *Ashley Madison's New Slogan: 'Find Your Moment,' Not 'Have an Affair*,*'* USA TODAY (July 12, 2016), http://www.usatoday.com/story/money/2016/07/12/ashley-madison-avid-media-ruby/86981490/.

10. *See* Tyler McCarthy, *Ashley Madison Hack Update: All the High Profile, Celebrity Names Attached to the Private Information Leak from the Cheating Website*, IBTIMES (Aug. 25, 2015, 8:24 AM), http://www.ibtimes.com/ashley-madison-hack-update-all-high-profile-celebrity-names-attached-private-2066211.

11. *See World's Biggest Data Breaches*, *supra* note 7; Tom Hamburger & Karen Tumulty, *WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations*, WASH. POST (July 22, 2016), http://wapo.st/29UbMp5?tid=ss_tw.

throughout her campaign.[12] Further, the U.S. intelligence community has concluded that the hack was tied to and possibly directed by the Russian government,[13] which sets a troubling precedent for future hacks by hostile foreign governments.

Plaintiffs whose information has been exposed due to a company data breach have attempted to sue the hacked companies storing their information based on causes of action such as negligence, breach of contract, unjust enrichment, breach of fiduciary duty, unfair and deceptive business practices, invasion of privacy, violation of the federal Fair Credit Reporting Act ("FCRA"), and violations of various state consumer protection and data breach notification laws.[14]

Data breach actions are expected to be the "next wave" of class actions.[15] Typically plaintiffs try to bring these claims as class actions because of the large number of plaintiffs and small amount of damages involved. Most data breach actions are brought in federal court based on the Class Action Fairness Act, 28 U.S.C. § 1332(d) (2012),[16] which extends federal diversity jurisdiction to all class actions in which minimal diversity exists and the amount in controversy exceeds $5 million.[17] However, courts dismiss a large portion of these data breach actions because plaintiffs lack a cognizable injury in fact, which is a requirement for Article III standing.

The Supreme Court has not yet set a uniform standard for what constitutes injury in the context of data breaches. As a result, there is a circuit split as to how much injury is sufficient. This split largely centers around whether increased risk of identity theft or fraud and, more recently, "sorting-things-out" costs[18] and monitoring expenditures[19] are sufficient to

12. Hamburger & Tumulty, *supra* note 11.

13. *Id.*

14. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690–91 (7th Cir. 2015); Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 959 (S.D. Cal. 2014); *In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, U.S. Dist. LEXIS 2592, at *2 (D. Minn. Jan. 7, 2016).

15. CARLTON FIELDS & JORDEN BURT, THE 2015 CARLTON FIELDS JORDEN BURT CLASS ACTION SURVEY 9 (2015), http://www.thenalfa.org/files/2015_Carlton_Class_Action_Survey.pdf.

16. *See, e.g.*, *Remijas*, 794 F.3d at 690.

17. Robin Miller, Annotation, *Construction and Application of Class Action Fairness Act of 2005*, *Pub. L. 109-2*, *119 Stat. 4 (2005)*, 18 A.L.R. Fed. 2d Art. I, § 1 (2007).

18. The costs associated with sorting things out are distinct from the purchase of monitoring services and generally encompass less easily calculable expenses, such as personal time expended canceling cards and ordering new ones, changing passwords or pin numbers, calling companies directly to verify suspicious communications received from them, closing banking accounts and opening new ones (if the bank account number was exposed), having a credit reporting agency place a fraud alert on one's account (if one's social security number was exposed), placing a credit freeze on one's account,

constitute an injury. But even if an action is dismissed in federal court for lack of Article III standing, it may succeed in state court, which is not subject to the Article III standing requirement.

In the realm of data breaches, technology is progressing rapidly; consequently, there is a lag time between the progress of technology and progress of the law. Because legislatures are slow to act and generally want a consensus to develop in the public or industry before writing protective measures into law, courts bear the burden of first impression, establishing a standard through case law on which the public can rely. This Note will offer a proposed standard for establishing injury under Article III's standing requirement in federal court. Part I provides background on the requirements of standing under Article III in the context of data breach cases. Part II discusses statutory standing and the effect of a recent Supreme Court statutory standing case on data breach litigation. Part III sets forth a proposed standard for recognizing injury in data breach cases. Part IV explores what effects this proposed standard would have on data breach litigation.

## I. BACKGROUND ON ARTICLE III STANDING IN DATA BREACH CASES

The Constitution establishes Article III standing as a "threshold question in every federal court case."[20] Article III standing requires a three-prong inquiry: to bring a suit in federal court, a plaintiff must suffer an injury that is (1) "concrete, particularized, and actual or imminent"; (2) "fairly traceable to the challenged action"; and (3) "redressable by a favorable ruling."[21] This Note will focus on the first prong, otherwise known as "injury in fact," in detail.

### A. FIRST PRONG: INJURY IN FACT

#### 1. Clapper v. Amnesty International USA

The Supreme Court has not directly addressed what constitutes an injury in data breach cases. Lower courts have largely had to rely on the Supreme Court case *Clapper v. Amnesty International USA* for guidance.

inserting new card information into one's auto-fill program, changing recurring payment methods, and communicating with banks. *What Should I Do If I Have Been a Victim of a Data Breach?*, TIME: MONEY, http://time.com/money/2791976/data-breach-victim/ (last visited Mar. 17, 2017).

19. Monitoring expenditures include expenditures on both credit monitoring and identity monitoring.

20. United States v. One Lincoln Navigator 1998, 328 F.3d 1011, 1013 (8th Cir. 2003).

21. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010) (citation omitted).

In *Clapper*, a group of attorneys and human rights, labor, legal, and media organizations, who allegedly had to have "sensitive and sometimes privileged telephone and e-mail communications" with individuals abroad for work, claimed there was an "objectively reasonable likelihood" that the Foreign Intelligence Surveillance Act would cause their communications to be monitored "at some point in the future."[22] However, there was no evidence that their communications had been targeted or that the government was going to target their communications.[23] Given this lack of evidence, the Court found plaintiffs' "theory of *future* injury . . . too speculative" and not actual or "certainly impending."[24] According to the Court, plaintiffs' allegations for standing were based on a "highly attenuated chain of possibilities."[25] The Court refused "to abandon [its] usual reluctance" to permit standing theories that rely on "speculation about the decisions of independent actors,"[26] rejecting the Second Circuit's "objectively reasonable likelihood" standard for establishing standing.[27] Further, plaintiffs' alleged injury of having "to take costly and burdensome measures to protect the confidentiality of their . . . communications" did not constitute standing because plaintiffs should not be able to "manufacture standing by incurring costs in anticipation of non-imminent harm."[28]

Courts have since used *Clapper* to dismiss data breach actions for failing to show a recognizable injury.[29] The majority of courts addressing data breach cases post-*Clapper* have required allegations of actual identity theft or fraud to establish an injury.[30]

2. Typical Injuries Alleged by Plaintiffs in Data Breach Actions

The injury in fact requirement tends to be the most difficult for plaintiffs in data breach cases to satisfy, and it is where courts' rulings vary the most. Plaintiffs have largely tried to allege injury through increased risk of identity theft or fraud, expenditures on sorting things out, and

22. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143–45 (2013).
23. *Id.* at 1147–50.
24. *Id.* at 1143, 1147 (citation and quotation marks omitted).
25. *Id.* at 1148.
26. *Id.* at 1150.
27. *Id.* at 1147.
28. *Id.* at 1143, 1155.
29. Christopher Browning, *Plaintiffs in IRS Data Breach Suits May Encounter Standing Challenges*, NIXON PEABODY (Aug. 31, 2015), http://web20.nixonpeabody.com/dataprivacy/Lists/Posts/Post.aspx?List=%201f414652-319f-47bd-a8de-5a649b6c4f12&ID=636.
30. *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 955 (D. Nev. 2015).

expenditures on monitoring services.[31]

3. Circuit Split

The Fourth Circuit recently recognized a split between the Sixth, Seventh, and Ninth Circuits and the First and Third Circuits over whether increased risk of identity theft or fraud is a qualifying injury for Article III standing.[32] The Sixth, Seventh, and Ninth Circuits have held that such a risk is sufficient to confer standing, while the First and Third Circuits have rejected such recognition of standing.[33] Additionally, the Sixth and Seventh Circuits have held that the cost of sorting things out and monitoring services qualify as cognizable injuries.[34] The Fourth Circuit chose not to follow the Sixth, Seventh, and Ninth Circuits.[35]

31. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 694 (7th Cir. 2015); *In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, 2016 U.S. Dist. LEXIS 2592, at *5 (D. Minn. Jan. 7, 2016). Plaintiffs also try to claim diminished value of their Personal Identifying Information ("PII") and overpayment for products; however, this Note will not address such injuries as courts have uniformly dismissed such allegations of injury. Absent allegations of attempts to sell one's PII and inability to do so, or forced acceptance of a lower price for one's PII, diminished value of PII does not constitute an injury. *SuperValu*, 2016 U.S. Dist. LEXIS 2592, at *20 (citing *Zappos.com*, 108 F. Supp. 3d at 954 ("finding no injury in fact where plaintiffs had not alleged that the data breach had prevented them from selling their personal information at the price it was worth")); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 30 (D.D.C. 2014) (same); Green v. eBay Inc., No. 14-1688, 2015 U.S. Dist. LEXIS 58047, at *20–21 n.59 (E.D. La. May 4, 2015) ("Even if the Court were to find that personal information has an inherent value and the deprivation of such value is an injury sufficient to confer standing, Plaintiff has failed to allege facts indicating how the value of his personal information has decreased as a result of the Data Breach."); Willingham v. Glob. Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *23 (N.D. Ga. Feb. 5, 2013) ("PII does not have an inherent monetary value."). Additionally, overpayment for products is a theory that "is consistently rejected in data breach cases where plaintiffs have not alleged that the value of the goods or services they purchased was diminished as a result of the data breach." *SuperValu*, 2016 U.S. Dist. LEXIS 2592, at *22. *See also id.* (citing *Zappos.com*, 108 F. Supp. 3d at 962 n.5 ("rejecting benefit-of-bargain theory where plaintiffs had not explained how the data breach impacted the value of the goods they purchased, and further had not alleged facts showing that the price plaintiffs paid for such goods incorporated a sum that both parties understood would be allocated towards the protection of customer data")); Fernandez v. Leidos, Inc., 127 F. Supp. 3d 1078, 1089 (E.D. Cal. Aug. 28, 2015) (finding no standing where plaintiff failed to allege facts from which a plausible inference could be drawn that the value of plaintiff's health care and insurance coverage had been diminished as a result of the data breach); *Remijas*, 794 F.3d at 694–95 (noting in dicta that the benefit-of-the-bargain theory was "problematic" and "dubious" where plaintiffs had not alleged any defect in any product they had purchased).

32. Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017).

33. *Id.*

34. Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388–89 (6th Cir. 2016); *Remijas*, 794 F.3d at 692, 696.

35. *Beck*, 848 F.3d at 276–77.

a. First and Third Circuits

The First and Third Circuits have only recognized injury in data breach cases where plaintiffs allege actual identity theft or fraud.[36] In *Storm v. Paytime, Inc.*, in which an unknown third party hacked a payroll processing company's computers, a class action lacked a cognizable injury because it failed to allege that any of the class action members experienced identity theft, had credit cards opened in their names, or had their bank accounts accessed as a result of the breach.[37] "In sum, their credit information and bank accounts [looked] the same . . . as they did prior to [the] data breach . . . ."[38] Thus, the court dismissed the action "without too much hesitation," as the Third Circuit requires dismissal in the absence of "actual misuse of the hacked data" or specific allegations "that such misuse is certainly impending."[39] Increased risk of identity theft alone is insufficient.[40] Moreover, the cost of sorting things out was rejected as an injury because the court saw it as a "prophylactic cost[]" that cannot be used to "manufacture standing" in the absence of data misuse.[41] Additionally, while the company offered a year of free credit monitoring and identity restoration services,[42] if it had not done so, and customers whose information was compromised had purchased monitoring services, the court would not have required the company to compensate the customers for the purchase in the absence of any actual identity theft.[43]

b. Ninth Circuit

Conversely, the Ninth Circuit has recognized increased risk of identity theft or fraud as an injury in data breach actions. In *Krottner v. Starbucks Corp.*, in which an employer's laptop computer containing the personal information of approximately 97,000 employees was stolen,[44] "an increase in the risk of identity theft [was] a constitutionally sufficient injury."[45] To establish injury in the Ninth Circuit, plaintiffs need only show a "credible

36. Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015).

37. *Storm*, 90 F. Supp. 3d at 363, 366.

38. *Id.* at 366.

39. *Id.* at 365, 367.

40. *Id.* at 365.

41. *Id.* at 367 (internal quotation marks omitted).

42. *Id.* at 364.

43. *See id.* at 368.

44. Krottner v. Starbucks Corp., No. C09-0216RAJ, 2009 U.S. Dist. LEXIS 130634, at *2 (W.D. Wash. Aug. 14, 2009), *aff'd*, 628 F.3d 1139 (9th Cir. 2010).

45. *Id.* at *12.

threat of harm" that is "both real and immediate."[46] By offering a monitoring service to employees subject to the breach, the defendant-employer was conceding "that some degree of monitoring [was] an appropriate response in the wake of the laptop theft."[47] If the employees had not suffered a present injury, their employer would not have offered them a present remedy.[48] Further, while the employees "might suffer *additional* injuries in the future, they [] already suffered (based on their allegations) an increase in their risk of identity theft."[49]

While courts in the D.C. Circuit have found *Clapper* to invalidate the Ninth Circuit's standard set out in *Krottner*,[50] courts in the Ninth Circuit have found *Krottner* to be compatible with *Clapper*.[51] In *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, in which gamers sued an online gaming provider over a criminal intrusion into the provider's database that stored gamers' Personal Identifying Information ("PII"),[52] gamers' allegations that their PII "was collected by [the provider] and then wrongfully disclosed as a result of the intrusion [were] sufficient to establish Article III standing" at the motion to dismiss stage.[53] None of the named plaintiffs needed to allege that their PII was used by the hacker; it was sufficient that plaintiffs "plausibly alleged a credible threat of impending harm based on the disclosure of their [PII] following the intrusion."[54] However, the gamers' subsequent purchase of credit monitoring was not a recognizable injury.[55] The provider offered free identity theft protection services,[56] but plaintiffs still tried to recover the

46. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (internal quotation marks omitted).

47. *Krottner*, 2009 U.S. Dist. LEXIS 130634, at *13.

48. *Id.*

49. *Id.* Despite finding that increased risk of identity theft was "not too speculative to constitute an injury in fact," *id.* at *18–19, thus granting the employees Article III standing, the court granted the employer's motion to dismiss because the employees were unable to establish an injury that Washington law recognized. *Id.* at *19, 30.

50. *E.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("[A]fter *Clapper*, . . . [a] 'credible threat of harm' standard is clearly not supportable.").

51. *E.g.*, *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 957 (D. Nev. 2015) ("*Krottner*'s phrasing is closer to *Clapper*'s 'certainly impending' language than it is to the Second Circuit's 'objectively reasonable likelihood' standard that the Supreme Court reversed in *Clapper*." (quoting *In re* Adobe Sys. Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014))).

52. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 953–54 (S.D. Cal. 2014).

53. *Id.* at 962.

54. *Id.* (citation and quotation marks omitted).

55. *Id.* at 970.

56. *Id.* at 955.

cost of purchasing their own credit monitoring.[57] The court found there were insufficient allegations that these "prophylactic costs" were "reasonably necessary, and therefore proximately caused by [the provider's] alleged breach," as there were no allegations of "instances of identity theft resulting from the intrusion."[58]

c. Seventh Circuit

The Seventh Circuit not only recognizes increased risk of identity theft or fraud as an injury, but it also recognizes the cost of sorting things out and monitoring services as injuries.[59] In *Remijas v. Neiman Marcus Group, LLC*, customers sued a luxury department store after hackers accessed the store's database containing customer credit card information.[60] While 9,200 customers actually experienced fraudulent charges, all had been reimbursed, and none alleged that their identities had been stolen.[61] Nevertheless, "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" established Article III standing as there were "identifiable costs associated with the process of sorting things out."[62] Additionally, "[p]resumably, the purpose of the hack [was], sooner or later, to make fraudulent charges or assume those consumers' identities."[63] And, going forward, there was a material factual dispute regarding bank reimbursement policies.[64] Thus, increased risk of identity theft and fraudulent credit- or debit-card charges constituted sufficiently imminent future injuries.[65] The court also said the cost of monitoring "easily qualifie[d] as a concrete injury."[66]

Following *Remijas*, the Seventh Circuit confirmed its position in *Lewert v. P.F. Chang's China Bistro, Inc.*, in which again, increased risk of identity theft or fraud, sorting-things-out costs, and credit monitoring expenses constituted cognizable injuries.[67] The purchase of credit monitoring qualified as an "easily quantifiable financial injury," and this

57. *Id.* at 970.
58. *Id.*
59. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 696 (7th Cir. 2015).
60. *Id.* at 689–90.
61. *Id.* at 692.
62. *Id.* at 692, 696.
63. *Id.* at 693.
64. *Id.* at 693–94.
65. *Id.* at 694.
66. *Id.*
67. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016).

time, monitoring services were not provided by the hacked company.[68] While no named plaintiffs incurred unreimbursed fraudulent charges, the court found "all class members should have the chance to show that they spent time and resources tracking down the possible fraud, changing automatic charges, and replacing cards as a prophylactic measure."[69]

d. Sixth Circuit

The Sixth Circuit has also recognized "allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, [as] sufficient to establish a cognizable Article III injury at the pleading stage."[70] In *Galaria v. Nationwide Mutual Insurance Co.*, hackers breached an insurance company's computer network and stole its customers' personal information.[71] The court found "[t]here is no need for speculation where [p]laintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."[72] Further, the insurance company recognized the severity of the risk by offering to provide credit monitoring and identity theft protection for a full year.[73] The court reasoned plaintiffs should not have to "wait for actual misuse . . . before taking steps to ensure their own personal and financial security."[74] Expending time and money to monitor credit, check bank statements, and modify financial accounts constituted an injury.[75] As did costs for monitoring services the insurance company recommended but did not cover and monitoring services the company offered for only a limited time where the risk was continuing.[76] The court found these costs to be "a concrete injury suffered to mitigate an imminent harm."[77]

The circuit split that has emerged as to what constitutes injury in data breach cases has been "troubling for businesses" that "had hoped, in the wake of *Clapper*, to receive some judicial relief from putative data breach class actions."[78] The Ninth Circuit and especially the Sixth and Seventh Circuits' "lenient view of Article III's standing requirement" appears to be

68. *See id.* at 969.
69. *Id.*
70. Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016).
71. *Id.* at 386.
72. *Id.* at 388.
73. *Id.*
74. *Id.*
75. *Id.* at 388–89.
76. *Id.*
77. *Id.* at 389.
78. Kristin Ann Shepard, *Circuit Split on Standing in Data Breach Class Actions Survives* Clapper, CARLTON FIELDS (Sept. 23, 2015), https://www.carltonfields.com/data-breach-class-actions-survives-clapper/.

marking these circuits as "emerging venue[s] of choice" for plaintiffs bringing data breach actions.[79] Moreover, state courts within the Seventh Circuit have rejected increased risk of identity theft or fraud as an injury,[80] making federal courts in the Seventh Circuit an even bigger target for data breach plaintiffs.

### B. SECOND PRONG: CAUSATION

The second element plaintiffs must show to establish standing is causation, meaning that an injury must be fairly traceable. "A showing that an injury is fairly traceable requires less than a showing of proximate cause. Even a showing that a plaintiff's injury is indirectly caused by a defendant's actions" is sufficient.[81] In data breach cases, this standing requirement has been satisfied where a business admits customer information has been exposed by issuing data breach notifications[82] or where a business issues new customer cards themselves due to a breach.[83] However, sometimes courts are reluctant to recognize causation in data breach cases. For example, in *Peters v. St. Joseph Services Corp.*, a patient who received a data breach notification from a health care service provider claimed that after the breach: (1) someone attempted to make a fraudulent purchase on her credit card that she used with the health care provider; (2) someone attempted to access her Amazon.com account using her son's name, which "could only have been obtained from names and next-of-kin information she provided to St. Joseph"; (3) she began receiving "daily telephone solicitations from medical products and services companies" asking "to speak with specific family members, whose contact information is recorded in her personal information"; and (4) her e-mail and mailing addresses had been compromised.[84] These incidents, which the patient identified "as evidence of actual identity theft/fraud," "fail[ed] to meet the causation and redressability elements of the standing test."[85] Specifically, the patient's claim lacked causation because she failed to "account for [a] sufficient break in causation caused by opportunistic third parties."[86]

79. *Id.*

80. *See, e.g.*, Maglio v. Advocate Health & Hosps. Corp., 40 N.E.3d 746, 753 (Ill. App. Ct. 2015).

81. Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012) (citation and quotation omitted).

82. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015).

83. *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 487 (D. Minn. 2015).

84. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 850–51 (S.D. Tex. 2015).

85. *Id.* at 857.

86. *Id.*

### C. THIRD PRONG: REDRESSABILITY

The final element plaintiffs must show to establish standing is redressability. "[I]t must be likely, as opposed to merely speculative, that [an] injury will be redressed by a favorable decision."[87] For example, in *Remijas*, this standing requirement was satisfied because compensation would be provided for "injuries caused by less than full reimbursement of unauthorized charges."[88] The court focused on mitigation expenses and future injuries, as all fraudulent charges had been reimbursed.[89] Conversely, in *Peters*, the patient's claimed injury lacked redressability because even if she obtained a favorable decision, she did not allege "any quantifiable damage or loss she [had] suffered as a result of the [d]ata [b]reach."[90] The patient never actually had to pay for any fraudulent charge on her credit card as she was able to decline approval, obtain a replacement card free of charge, and close her account to prevent future fraud.[91] Furthermore, after changing her e-mail password, fraudulent account activity ceased.[92] Finally, the court was unable to "prevent medical products and services companies from contacting [her] or otherwise disgorge them of her personal information."[93]

Out of the three prongs of Article III standing that data breach plaintiffs must satisfy, plaintiffs most often falter on establishing injury, and this is where the predominant circuit split has emerged. Thus, establishing a uniform theory of injury will be the focal point of this Note.

## II. STATUTORY STANDING

Data breach plaintiffs often attempt to satisfy Article III standing through alleging statutory standing. Statutory standing refers to "legislatively-created causes of action . . . . [I]t asks whether a statute creating a private right of action authorizes a particular plaintiff to avail herself of that right of action."[94] In May 2016, the Supreme Court stated in *Spokeo, Inc. v. Robins* that evidence of a statutory violation alone will not

87. Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992) (citation and quotation marks omitted).
88. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).
89. *Id.* at 696–97.
90. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015).
91. *Id.* at 850–51.
92. *Id.* at 857.
93. *Id.* ("Certainly, the Court can neither 'control [n]or . . . predict' the 'unfettered choices' made by these companies, who are not before the Court and are independent of [the health care service provider] in any event." (citation omitted)).
94. Radha A. Pathak, *Statutory Standing and the Tyranny of Labels*, 62 OKLA. L. REV. 89, 91 (2010).

automatically satisfy Article III's injury requirement.[95] Supreme Court precedent has long been inconsistent in recognizing statutory standing. While it might be assumed that the Court's clarification in *Spokeo* would eliminate federal data breach actions that rely on statutory violations to establish injury, the Third, Sixth, and Eleventh Circuits have found statutory violations to constitute a cognizable injury in data breach cases post-*Spokeo*.[96]

### A. *SPOKEO, INC. V. ROBINS*

In *Spokeo*, a people-search website that accumulates personal information about people, such as their address, phone number, e-mail address, and family members, contained false information.[97] A site user claimed to have suffered reputational, economic, and emotional injuries when the website described him as wealthier and better educated than he was.[98] The user claimed the inaccuracies violated the FCRA, which provides individual damages ranging between one hundred and one thousand dollars.[99] In addition to his own payout, the user sought to represent a class consisting "of millions of individuals, and he want[ed] each to get the maximum payout under the FCRA."[100] Although the district court dismissed the case, the Ninth Circuit found standing in "simply alleging the violation of the FCRA."[101] The Supreme Court granted certiorari[102] and remanded the case due to an incomplete analysis of Article III standing.[103] While the Ninth Circuit analyzed the particularity

95. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.").

96. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 629 (3d Cir. 2017) ("[A] violation of FCRA gives rise to an injury sufficient for Article III standing purposes. Even without evidence that the Plaintiffs' information was in fact used improperly, the alleged disclosure of their personal information created a *de facto* injury."); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 391 (6th Cir. 2016); Church v. Accretive Health, Inc., 654 Fed. App'x 990, 995 (11th Cir. 2016).

97. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1544 (2016).

98. *Id.* (Ginsburg, J., dissenting).

99. *Id.* at 1545.

100. *Inventing Class Actions*, WALL STREET J. (Nov. 1, 2015, 5:21 PM) (quotations omitted), http://www.wsj.com/ articles/inventing-class-actions-1446416470.

101. *Id.*

102. Spokeo, Inc. v. Robins, 135 S. Ct. 1892, 1892 (2015).

103. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016).

requirement of the plaintiff's injury, the Supreme Court found that it failed to analyze the concreteness of the alleged injury.[104] But more importantly, in remanding the case, the Court rejected a statute's ability to confer Article III standing in the absence of a cognizable injury.[105]

### B. HISTORICAL DIVIDE IN RECOGNIZING STATUTORY STANDING

Since the landmark case *Lujan v. Defenders of Wildlife*, in which wildlife conservation organizations lacked standing to challenge the Secretary of the Interior's new interpretation of the Endangered Species Act ("ESA"),[106] there has consistently been a 5–4 split in the Court as to how much injury a plaintiff must allege to warrant federal jurisdiction—reflecting an underlying disagreement among Justices at two levels: first, the scope of federal jurisdiction generally, and second, whether a particular claim is of sufficient import to invoke federal jurisdiction.

#### 1. Arguments Against Statutory Standing

Arguments that Congress should not be able to manufacture standing largely rest on the idea that it would violate Article III of the Constitution. "[T]he requirement of injury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute."[107] "If plaintiffs can get by on a statutory violation, they don't all need to show actual harm, let alone the same harm [in a class action]."[108]

There is a strong line of Supreme Court cases rejecting Congress's ability to confer statutory standing where there is no recognizable injury. In *Lujan*, wildlife conservation organizations attempted to sue the Secretary of the Interior under the "citizen-suit" provision of the ESA, which provided that "any person may commence a civil suit on his own behalf . . . to enjoin any person" allegedly violating the ESA.[109] The Court held that a "congressional conferral upon *all* persons of an abstract, self-contained, noninstrumental 'right' to have the Executive observe the procedures required by law" does not satisfy the injury requirement;[110] rather, a "factual showing of perceptible harm" is required.[111] "[T]he President, not the courts, holds the power to execute legislative policy"; statutory

104. *Id.*
105. *Id.* at 1550.
106. Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992).
107. Summers v. Earth Island Inst., 555 U.S. 488, 497 (2009).
108. *Inventing Class Actions*, *supra* note 100.
109. *Lujan*, 504 U.S. at 571–72 (citation omitted).
110. *Id.* at 601 (Blackmun, J., dissenting) (describing the Court's conclusion).
111. *Id.* at 566.

conferral of standing would require the judiciary to encroach upon the executive's "enforcement prerogatives."[112] But the Court did note that this was not a situation in which Congress provided a "cash bounty" for private plaintiffs, which would have created "a concrete private interest in the outcome of a suit against a private party for the Government's benefit."[113]

Additionally, in *Whitmore v. Arkansas*, in which a third party lacked Article III standing to challenge the constitutionality of a death sentence imposed on a capital defendant under the Eighth and Fourteenth Amendments,[114] the Court reasoned that the "threshold inquiry into standing 'in no way depends on the merits of the [third party's] contention that particular conduct is illegal.'"[115] The third party simply raised a "generalized interest of all citizens in constitutional governance," which is insufficient for Article III standing.[116] An alleged harm must be "distinct and palpable," not "abstract," "conjectural," or "hypothetical."[117] Also, in *Allen v. Wright*, in which parents of black public school children lacked Article III standing to challenge the Internal Revenue Service's failure to consistently deny tax-exemption status to racially discriminatory private schools,[118] the Court reasoned that "a claim simply to have the Government avoid the violation of law" is not a "claim of injury judicially cognizable."[119] Rather, plaintiffs must suffer "actual present or immediately threatened injury resulting from unlawful governmental action."[120]

2. Arguments Supporting Statutory Standing

Arguments that Congress should be able to manufacture standing by enabling individuals to sue for statutory damages where injury would otherwise not exist largely rest on the separation-of-powers doctrine. These arguments follow the line of reasoning that the Court's job "is to preserve and protect congressional primacy in lawmaking," as that is what statutory

112. Maxwell L. Stearns, Spokeo, Inc. v. Robins *and the Constitutional Foundations of Statutory Standing*, 68 VAND. L. REV. EN BANC 221, 232 (2015).

113. *Lujan*, 504 U.S. at 573.

114. Whitmore v. Arkansas, 495 U.S. 149, 151 (1990).

115. *Id.* at 155 (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)).

116. *Id.* at 160 (citing Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 217 (1974)).

117. *Id.* at 155 (citing Laird v. Tatum, 408 U.S. 1, 15 (1972)).

118. Allen v. Wright, 468 U.S. 737, 739–40 (1984).

119. *Id.* at 753–54.

120. *Id.* at 760 (citation omitted).

standing doctrine is designed to do.[121] "A logical first step is deferring when Congress chooses who has standing to enforce its statutes."[122]

Despite the strong line of cases declining to recognize statutory standing, there are other Supreme Court cases post-*Lujan* in which the 5–4 split has come out the other way. For example, in *Massachusetts v. EPA*, in which environmental organizations and state and local governments had Article III standing to challenge an Environmental Protection Agency order declining to regulate new motor vehicles' greenhouse gas emissions under Section 202 of the Clean Air Act,[123] the Court found that "[t]he parties' dispute turn[ed] on the proper construction of a congressional statute, a question eminently suitable to resolution in federal court."[124] Furthermore, under 42 U.S.C. § 7607, Congress authorized such a petition for review despite the absence of a cash-bounty provision.[125]

In addition, in *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, in which environmentalists had Article III standing to sue a hazardous waste facility for violating the Clean Water Act ("CWA"),[126] the Court reasoned that "a company's continuous and pervasive illegal discharges of pollutants into a river [could] cause nearby residents to curtail their recreational use of that waterway and . . . subject them to other economic and aesthetic harms," constituting an injury.[127] Here, as in *Lujan*, environmentalists used a "citizen-suit" provision, this time under the CWA, to allege standing.[128] The provision permitted the award of "appropriate civil penalties."[129]

Also, in *FEC v. Akins*, in which voters had Article III standing to challenge the Federal Election Commission's determination that the American Israel Public Affairs Committee was not subject to disclosure requirements under the Federal Election Campaign Act of 1971

121. Stearns, *supra* note 112, at 222. *But see* Lujan v. Defs. of Wildlife, 504 U.S. 555, 577 (1992) (noting a separation-of-powers concern where statutes permit citizens to bring suit against executive officers) ("To permit Congress to convert the undifferentiated public interest in executive officers' compliance with the law into an 'individual right' vindicable in the courts is to permit Congress to transfer from the President to the courts the Chief Executive's most important constitutional duty . . . .").

122. Stearns, *supra* note 112, at 241.

123. Massachusetts v. EPA, 549 U.S. 497, 510, 514, 526 (2007).

124. *Id.* at 516.

125. *Id.*

126. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 174–76 (2000).

127. *Id.* at 184–85.

128. *Id.* at 173.

129. *Id*.

("FECA"),[130] the Court reasoned that such an "informational injury" that "directly related to voting, the most basic of political rights," was "sufficiently concrete and specific" that its widespread effect did "not deprive Congress of constitutional power to authorize its vindication in the federal courts."[131] Under the FECA, Congress provided that anyone may file a complaint alleging a violation of the FECA with the Commission;[132] should that complaint be dismissed, the complainant may file a petition in district court seeking review.[133] The statute provided fines for violators of the FECA, but not a cash bounty for victorious private plaintiffs.[134]

### C. IMPACT OF *SPOKEO* ON DATA BREACH CASES

Despite the Court's ruling in *Spokeo*, federal appeals courts have since found statutory violations sufficient to constitute injury for Article III standing.[135] For example, in *In re Horizon Healthcare Services Inc. Data Breach Litigation*, two laptop computers containing customers' personal information were stolen from a health insurer.[136] The plaintiffs alleged the insurer inadequately protected their information in violation of the FCRA.[137] While the district court dismissed the case for lack of Article III standing, the Third Circuit found that "a violation of [the] FCRA gives rise to an injury sufficient for Article III standing purposes."[138] The alleged disclosure of plaintiffs' personal information "created a *de facto* injury" regardless of whether their "information was in fact used improperly."[139] The Third Circuit found this to be compatible with *Spokeo*, finding that the Court did not intend "to change the traditional standard for the establishment of standing."[140] In sum, while *Spokeo* may have appeared to set a firm precedent for statutory standing, the recent federal appeals courts' decisions granting statutory standing show the historical divide will likely persist.

130. FEC v. Akins, 524 U.S. 11, 13–14 (1998).
131. *Id.* at 24–25.
132. 52 U.S.C. § 30109(a)(1) (2012).
133. *Id.* § 30109(a)(8)(A).
134. *Id.* § 30109(d).
135. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 629 (3d Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 391 (6th Cir. 2016); Church v. Accretive Health, Inc., 654 Fed. App'x 990, 995 (11th Cir. 2016).
136. *In re Horizon Healthcare Servs. Inc.*, 846 F.3d at 629.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.* at 636–38.

## III. PROPOSED STANDARD FOR ESTABLISHING INJURY IN FACT IN DATA BREACH CASES

Where a data breach occurred because of a defendant's lapse, the Supreme Court can best provide a remedy for plaintiffs by recognizing standing where actual, unremedied identity theft or fraud is alleged and where one has reasonably invested in monitoring services. A mere increased risk of identity theft or fraud should not suffice. If the Court was inclined to go further, it could additionally recognize standing for reasonable and substantial sorting-things-out costs, but in reality such a recognition of standing is likely impractical.

### A. ACTUAL, UNREMEDIED IDENTITY THEFT OR FRAUD SHOULD BE A COMPENSABLE INJURY

For alleged theft or fraud to be compensable, actual identity theft or fraud should have occurred *and* a plaintiff should have sustained some actual loss from that theft or fraud—for example, a fraudulent charge was made to a plaintiff's card that the plaintiff's card issuer refused to reimburse.

#### 1. Only Unremedied Costs Should Be Compensable

Where fraud has been alleged, but has been remedied, as in *Remijas*,[141] plaintiffs suffer no real injury or harm. Thus, reimbursed fraudulent charges should not constitute an injury.

The only times fraud should constitute an injury is if it has not been remedied or the plaintiff incurred some financial burden from the fraud, as in *In re Target Corp. Customer Data Security Breach Litigation*.[142] In *In re Target*, in which hackers accessed credit cards, debit cards, and other PII of 110 million Target customers during the 2013 holiday season, the plaintiff-customers alleged "that they actually incurred unauthorized charges; lost access to their accounts; and/or were forced to pay sums such as late fees, card-replacement fees, and credit monitoring costs because the hackers misused their personal financial information."[143] Such sustained expenses should comprise a compensable injury, and the Eighth Circuit district court agreed in *In re Target*.[144]

141. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692 (7th Cir. 2015).

142. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. 2014).

143. *Id.* at 1157–58.

144. *Id.* at 1158–59.

Recognizing injury only where plaintiffs have incurred actual, unremedied costs would result in more accurate and fair damages and reduce overlap in damages between financial institutions and individual plaintiffs. Otherwise, plaintiffs would be overcompensated, and hacked companies would be paying double damages—both to individuals and to the financial institutions that are reimbursing the fraudulent charges.[145] Considering the facts in the recent *Remijas* case—that despite 9,200 customers incurring fraudulent charges, none went unreimbursed[146]—such a result seems likely should courts force companies to compensate plaintiffs before they sustain any actual loss.

2. Compensating Mere Increased Risk of Identity Theft or Fraud Would Result in Inaccurate and Unfair Damages

"[C]ourts cannot be in the business of prognosticating whether a particular hacker [is] sophisticated or malicious enough to both be able to successfully read and manipulate [stolen] data and engage in identity theft."[147] Even if plaintiffs were able to obtain a favorable judgment based on increased risk of identity theft or fraud, that judgment would not prevent an unknown third-party hacker from thereafter making use of the stolen information, similar to how in *Peters*, the court admittedly could not stop solicitations the patient had been receiving from medical products and services companies.[148] Before any actual, unremedied theft or fraud has occurred, courts can only provide compensation for anticipated damages. To do that, courts first have to speculate as to whether theft or fraud might happen, and then, speculating that it will happen, speculate further as to what potential damages might result. Hence, damages based on increased risk of identity theft or fraud are too difficult to calculate ex ante, and it is unfair to force companies to pay for such speculative damages before they occur.

Courts that have refused to recognize increased risk of identity theft or fraud as an injury have told plaintiffs that "once a third party misuses a person's personal information," that person "would be free to return to

145. *See In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 484–85 (D. Minn. 2015).

146. *Remijas*, 794 F.3d at 692.

147. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 368 (M.D. Pa. 2015).

148. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) ("Certainly, the Court can neither 'control [n]or . . . predict' the 'unfettered choices' made by these companies, who are not before the Court and are independent of [the health care service provider] in any event." (citation omitted)).

court and would have standing to recover her losses."[149] While these courts did not address how this would affect any statute of limitations, under the proposed standard of this Note, the applicable statute of limitations would not begin to run against that person until actual, unremedied identity theft or fraud occurs. The same would be true of class action members who might prefer to wait and see if they experience any actual, unremedied identity theft or fraud, and then seek the full amount of their actual loss, as long as they opt out of the class action upon receiving notice of class certification.[150] Typically, if a data breach class action survives a motion to dismiss, it will end up settling; such settlement agreements generally provide extremely broad settlement releases, preventing any class action member from bringing future claims should, for example, unremedied identity theft or fraud thereafter occur from the data breach in question.[151] These broad settlement releases are enforceable.[152]

One of the problems with allowing plaintiffs to seek relief at a later point is that causation may be difficult to prove. Should any actual identity theft or fraud occur as a result of a data breach, it is likely to occur relatively close to the time of the breach. As will be discussed in Part III.B.1, the amount of time a victim is truly at risk is approximately one year. For example, in *Remijas*, the 9,200 customers who alleged actual fraud all experienced it within six months of the data breach.[153] However, it may be possible for plaintiffs to establish that the risk is continuing.[154] But data breach victims will presumably protect against future fraud by changing exposed passwords, replacing exposed bank cards, and closing exposed bank accounts and opening new ones, for which they could

149. *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 961–62 (D. Nev. 2015) (quoting *Storm*, 90 F. Supp. 3d at 367).

150. As long as an individual opts out of a class action upon receiving notification of class certification, that person is no longer a member of that class. FED. R. CIV. P. 23(b)(3); FED. R. CIV. P. 23(c)(2)(B)(v); FED. R. CIV. P. 23(e)(4). *See also* WILLIAM B. RUBENSTEIN, NEWBERG ON CLASS ACTIONS § 13:23, n.4, n.5 (5th ed.).

151. *See, e.g.*, Class Action Settlement Agreement at 1, 11–12, 27–28, Curry v. AvMed, Inc., No. 10–cv–24513–JLK, 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Oct. 21, 2013). *See also* Andrew S. Tulumello & Mark Whitburn, *Res Judicata and Collateral Estoppel Issues in Class Litigation*, *in* A PRACTITIONER'S GUIDE TO CLASS ACTIONS 605, 614 (Marcy Hogan Greer ed., 2010) ("Class action litigants may release claims through settlement even if the named plaintiffs never had standing to bring the released claims or the claims were not ripe at the time of settlement. Moreover, claims can be released even if they were not pursued by the named plaintiffs at all or are asserted against parties not named as defendants in the settled action.").

152. Tulumello & Whitburn, *supra* note 151, at 614.

153. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

154. *See* Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388–89 (6th Cir. 2016) (recognizing plaintiffs' expenditures on monitoring services as an injury where the risk of identity theft or fraud was continuing and the defendant only provided monitoring services for one year).

potentially seek compensation under Part III.C of this Note.

3. Consistency with *Clapper*

Denying standing for increased risk of identity theft or fraud is consistent with *Clapper*, in which an increased risk that plaintiffs' communications would be monitored in the future was insufficient to confer standing.[155] Both increased risk of monitoring in *Clapper* and increased risk of identity theft or fraud in data breach cases rest on a "highly attenuated chain of possibilities" involving "speculation about the decisions of independent actors."[156] Recognizing an injury for increased risk of identity theft or fraud requires overcoming a string of "*if*s": only "*if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully,"[157] and *if* unremedied costs result from the fraud would there be a compensable injury.

## B. MONEY SPENT ON MONITORING SERVICES SHOULD BE COMPENSABLE

Money spent on monitoring services results in a concrete, particularized, and redressable injury, and it should be compensated as such, so long as the costs are reasonable. Therefore, failure of a hacked company to reasonably provide customers with monitoring services should constitute a cognizable injury.

1. Reasonableness

It would be reasonable to invest in monitoring services and expend time sorting things out (discussed in Part III.C) as long as customers have been informed of a breach affecting their sensitive information and have no reason to believe that insufficient information was accessed for any real harm to come from the breach. In 2015, one in five customers who received notification of a data breach became a victim of fraud.[158] In 2014, it was one in seven.[159] Moreover, "[f]orty-six percent of consumers with breached debit cards in 2013 became fraud victims in the same year."[160] As the Sixth

155. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

156. *Id.* at 1148, 1150.

157. Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (plaintiffs lacked standing).

158. *13.1 Million Identity Fraud Victims but Less Stolen in 2015, According to Javelin*, JAVELIN STRATEGY (Feb. 2, 2016), https://www.javelinstrategy.com/press-release/131-million-identity-fraud-victims-less-stolen-2015-according-javelin.

159. *Id.*

160. *A New Identity Fraud Victim Every Two Seconds in 2013, According to Javelin*, JAVELIN

Circuit reasoned in *Galaria v. Nationwide Mutual Insurance Co.*, "it would be unreasonable to expect Plaintiffs to wait for actual misuse . . . before taking steps to ensure their own personal and financial security."[161]

While breach notification laws may not be perfect, and it may not be possible for companies to know the exact number of victims whose records have been compromised, for practicality purposes, should a person receive a breach notice from a company, there is a sufficient likelihood that the person's records were exposed, such that the person could reasonably invest in monitoring services and expend time sorting things out. Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutes requiring individual notifications after a security breach involving PII.[162] These notification statutes "typically have provisions regarding . . . what constitutes a breach . . . [and] who must be notified . . . and exemptions (e.g., for encrypted information)."[163] Moreover, forty-one states "require analysis of a breach's risk-of-harm as a prerequisite for determining whether notification is required."[164]

In *Remijas*, the Seventh Circuit suggested on remand that the district court "look into [the] length of time that a victim is truly at risk; the GAO [Government Accountability Office] suggests at least one year, but more data may shed light on this question."[165] This Note takes the position that one year of monitoring is presumptively reasonable, but plaintiffs may rebut that presumption with evidence that the risk of identity theft or fraud is continuing.[166]

2. Distinguishing From *Clapper*

Unlike in *Clapper*, in which there was merely a threatened wrong that plaintiffs' communications would be monitored, in the context of data breaches, a wrong has already occurred in the form of a breach. Additionally, unlike in *Clapper*, in which there was no evidence that the

STRATEGY (Feb. 5, 2016), https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy.

161. Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016).

162. *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Feb. 24, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

163. *Id.*

164. Rachael M. Peters, Note, *So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1183 (2014) (citation omitted).

165. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).

166. *See Galaria*, 663 Fed. App'x at 388–89 (recognizing plaintiffs' expenditures on monitoring services as an injury where the risk of identity theft or fraud was continuing and the defendant only provided monitoring services for one year).

government had been spying on the plaintiffs, here receiving notification of a breach affecting one's personal information is sufficiently probative to establish that a person's data has been compromised. In *Remijas*, the Seventh Circuit found the customers' situation to be different from the plaintiffs' situation in *Clapper* because "there [was] no need to speculate as to whether the . . . [customers' information was] stolen and what information was taken."[167] Reasonable responses to a breach will incur costs, and those costs should be compensated so long as the breach occurred because of a defendant's lapse. Thus, purchasing monitoring services after a breach has already occurred is not the kind of manufactured injury that *Clapper* rejected.[168]

3. Justifying Compensation for Monitoring Services by Looking at Other Areas of Law

Compensating plaintiffs for monitoring services is also justified by looking at existing models in other areas of law, such as the "duty to mitigate" doctrine in contracts and the recognition of medical monitoring as a remedy in torts.

a. Duty to Mitigate

The same policy behind the duty to mitigate in contracts supports encouraging plaintiffs' purchase of monitoring services in data breaches. Courts have recognized that "a plaintiff may 'recover for costs and harms incurred during a reasonable effort to mitigate,' regardless of whether the harm is nonphysical."[169] In contracts, the duty to mitigate encourages plaintiffs to take reasonable measures to avoid unnecessary increases in damages by not awarding plaintiffs damages that are avoidable and unnecessary.[170] In data breaches, typically breached companies offer free monitoring services to customers subject to a breach,[171] but if a company were to fail to provide monitoring services, responsible plaintiffs who purchased monitoring services to mitigate potential damages should be compensated for their purchase. The Sixth, Seventh, and Ninth Circuits

167. *Remijas*, 794 F.3d at 693 (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).

168. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013).

169. Anderson v. Hannaford Bros., 659 F.3d 151, 162 (1st Cir. 2011) (quoting *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010)).

170. 11 JOSEPH M. PERILLO, CORBIN ON CONTRACTS § 57.11 (2005).

171. *See, e.g.*, Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 364 (M.D. Pa. 2015); Petition for Rehearing En Banc at 5, *Remijas*, 794 F.3d 688 (No. 14-3122) (noting that Neiman Marcus voluntarily supplied its customers with one year of free credit monitoring and identity theft protection).

have already acknowledged the appropriateness of hacked companies offering free monitoring services in the wake of a data breach.[172] Credit and identity monitoring can lead to the discovery of harm before too much damage, or any damage, is done, reducing the total damages—an economically efficient goal.

b. Medical Monitoring

Courts often analogize the recoverability of monitoring services in data breach actions to medical monitoring in tort actions.[173] Similar to seeking compensation for medical monitoring to avoid or mitigate injuries from a known exposure to a toxic substance, plaintiffs in data breach actions seek monitoring services to avoid or mitigate damages from a known security breach.[174] Through breach notifications, companies are admitting that plaintiffs have been exposed.

Federal appeals courts and lower courts have "analyzed medical monitoring claims without expressing any concern about standing."[175]

> Since the landmark decision *Askey v. Occidental Chemical Corp*., . . . [176] in which a New York appeals court acknowledged medical monitoring could be a recoverable damage, appellate courts in at least ten other states have recognized claims for medical monitoring. In addition, federal courts have interpreted state law in at least seven additional states

172. *Remijas*, 794 F.3d at 694 ("It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."); Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016) ("Nationwide seems to recognize the severity of the risk, given its offer to provide credit monitoring and identity theft protection for a full year."); Krottner v. Starbucks Corp., No. C09-0216RAJ, 2009 U.S. Dist. LEXIS 130634, at *12 (W.D. Wash. Aug. 14, 2009), *aff'd*, 628 F.3d 1139 (9th Cir. 2010) ("Starbucks apparently concedes that some degree of monitoring is an appropriate response in the wake of the laptop theft, because it has offered a monitoring service to affected employees.").

173. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014).

174. *Krottner*, 2009 U.S. Dist. LEXIS 130634, at *15 ("Plaintiffs facing an increased risk of identity theft are similar in some respects to plaintiffs seeking medical monitoring as a remedy for an increased risk of disease or injury, and no federal court has used Article III to close the courthouse doors to a medical monitoring claim.").

175. *Id.* at *16–17.

176. Askey v. Occidental Chem. Corp., 477 N.Y.S.2d 242 (App. Div. 1984), *superseded by rule*, N.Y. C.P.L.R. § 214-c (McKinney 2017) (superseding *Askey*'s "accrual rule" and limiting medical monitoring claims to three years "from the date of discovery of injury by the plaintiff or from the date when through the exercise of reasonable diligence such injury should have been discovered by the plaintiff, whichever is earlier").

> and the District of Columbia as permitting claims for medical monitoring.[177]

Courts are more inclined to recognize medical monitoring as a remedy than as a cause of action.[178] Under the proposed standard of this Note, monitoring services would not constitute a cause of action, but rather a recognizable injury.

As for medical monitoring requests in the context of class certification, in a recent class action college basketball players requested a medical monitoring program to enable them to monitor whether they had "any long-term effects or neurodegenerative conditions related to concussions or subconcussive hits."[179] The court found that the medical monitoring program was "designed to relieve class plaintiffs of the prospective costs associated with medical supervision" and was therefore "amenable to certification under Rule 23(b)(2)."[180]

c. Mitigating Damages

If a hacked company provides reasonable, effective[181] monitoring services for at least one year or if it would not be reasonable for a plaintiff to purchase monitoring services, damages would be reduced as there would presumptively not be a compensable injury. In addition, a hacked company will only ever be liable if it was at fault in some way for the hack (e.g., was negligent).

### C. EXPENDITURES ON SORTING THINGS OUT COULD POTENTIALLY BE COMPENSABLE

Where expenditures on sorting things out are reasonable[182] and substantial, such expenditures can be distinguished from other forms of injury that data breach plaintiffs allege, namely increased risk of identity theft or fraud. If the Court were inclined to expand standing doctrine in

177. Badillo v. Am. Brands, 16 P.3d 435, 438–39 (Nev. 2001).

178. *Id.* at 440.

179. *In re* NCAA Student-Athlete Concussion Injury Litig., 314 F.R.D. 580, 599 (N.D. Ill. 2016).

180. *Id.* at 602 n.27.

181. In the context of this Note, monitoring services would be ineffective where only credit monitoring is provided and not identity monitoring, or vice versa; where a plaintiff purchases a monitoring service privately that flags fraudulent activity that the complimentary service does not; or where the complimentary service does not cover a service that the hacked company recommends. *See, e.g.*, Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388–89 (6th Cir. 2016) (recognizing an injury for costs to obtain protections that the defendant recommended but did not cover).

182. *See* discussion *supra* Part III.B.1.

data breach cases, recognizing expenditures on sorting things out as an injury would be an ideal way to do so.

1. Defining Sorting-Things-Out Costs

Potential sorting-things-out costs could include time expended canceling bank cards and ordering new ones, changing passwords or pin numbers, calling companies directly to verify suspicious communications received from them, closing bank accounts and opening new ones (if the bank account number was exposed), having a credit reporting agency place a fraud alert on one's account (if one's social security number was exposed), placing a credit freeze on one's account, inserting new card information into one's auto-fill program, changing recurring payment methods, and communicating with banks.[183] What would not be included is reviewing one's financial statements; reasonably prudent people will examine their statements on a regular basis regardless of a breach.

2. Substantiality

The range of time and resources spent sorting out one's finances after a breach can vary greatly. More than half (52%) of the 17.6 million identity theft victims in 2014 "were able to resolve any problems . . . in a day or less, while about 9% spent more than a month."[184] Another statistic shows that "[d]ata breach victims spend an average of 41 hours on resolution."[185]

Compensating insubstantial expenditures on sorting things out would likely result in an unjustified use of resources when accounting for the cost of attorneys' fees. Because of the potential for exorbitant attorneys' fees to overshadow the damages of minimal sorting-things-out expenses, there should be a threshold amount of time that must be expended for such an injury to be compensable. For example, the majority of 2014 identity theft victims who were able to resolve any problems in a day or less would not qualify, but the 9% who spent more than a month potentially would.

In *Storm v. Paytime, Inc.*, one plaintiff was an employee of a government contractor and was required to have security clearances to perform his job.[186] After a data breach, the employee "reported the incident to [his] employer, who then suspended his security clearances while the

183. *What Should I Do If I Have Been a Victim of a Data Breach?*, *supra* note 18.

184. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ248991, VICTIMS OF IDENTITY THEFT, 2014 (2015), http://www. bjs.gov/content/pub/pdf/vit14_sum.pdf.

185. *Top Articles on Data Breaches*, LIFELOCK, https://www.lifelock.com/education/identity-theft-news/data-breaches/ (last visited Mar. 22, 2017).

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

employer investigated the situation. During the investigation, [the employee] was required to work at a different job site, resulting in a four hour increase in his daily commute."[187] This injury was a direct result of the actual, non-speculative *breach*, not any identity theft or fraud. While the Third Circuit district court did not recognize the employee's costs as an injury,[188] this type of injury, resulting exclusively from the occurrence of a breach, would potentially be compensable under sorting-things-out costs, depending on how long he was required to work at the alternate job site.

3. Compensation for Time Expended in Other Torts

In other torts, time expended in pursuit of a solution is compensated. In conversions, for example, damages may include time and money lost in pursuit of a property as long as such expenditures are reasonable and not excessive.[189]

In general, if someone's tort threatens the legally protected interests of another, the victim may "recover for expenditures reasonably made . . . to avert the harm threatened."[190] And if someone has suffered injury from another person's tort, the victim may "recover for expenditures reasonably made . . . to avert further harm."[191] Thus, in data breaches, where a company's lapse has resulted in a third party's ability to gain access to a customer's sensitive information, the customer should be able to recover for expenditures reasonably made to avert the threatened harm of identity theft or fraud.

4. Mitigating Damages

The cost of sorting things out is mitigated where card issuers independently replace customers' cards due to a breach as this reduces the time customers might otherwise have to spend sorting things out.

Moreover, encouraging customers to sort things out will reduce overall damages. If customers notify their card issuer of a breach with reasonable promptness, it will minimize (1) the potential for fraudulent charges to be approved and (2) their liability for the fraudulent charges.

187. *Id.* (citation omitted).

188. *Id.* at 368.

189. CONRAD L. RUSHING ET AL., MATTHEW BENDER PRACTICE GUIDE: CALIFORNIA UNFAIR COMPETITION AND BUSINESS TORTS § 7.16 (2016) (citing CAL. CIV. CODE § 3336 (West 2016) and Haines v. Parra, 239 Cal. Rptr. 178 (Ct. App. 1987)).

190. RESTATEMENT (SECOND) OF TORTS § 919(1) (AM. LAW INST. 1979).

191. *Id.* § 919(2).

With respect to credit cards, if customers notify their credit card issuer that their credit card has been compromised before fraud occurs, customers will not be responsible for any charges they did not authorize. If customers fail to notify their credit card issuer, their liability may reach $50.[192] On the other hand, with debit cards, if customers fail "to report to [their] bank that money has been taken from [their] debit card account more than 60 days after [they] receive[] the statement, there is no limit to [their] liability and [they] could lose all the money in [their] account."[193] While these mitigation efforts may, in part, shift defendants' liability from customers to banks, by alerting banks to the potential for fraudulent activity, they may reduce banks' damages from the breach.

Again, where hacked companies have exercised the requisite level of care, they will not be held responsible for the actions of unknown third-party hackers. It is quite plausible that there is no real fault on behalf of the companies because hacking technology is progressing so rapidly that companies cannot reasonably be expected to keep up defensively.

5. Accounting for Variable Sorting-Things-Out Costs in Class Action Settlements

Because of the small amount of monetary damages involved, data breach actions are generally only viable if they can qualify for class action status. Thus, class certification is key. While the cost of sorting things out is likely to vary significantly from person to person, this kind of variability is typical in class actions and should not prohibit class certification. *In re Currency Conversion Fee Antitrust Litigation* exemplifies a typical way this variability is handled.

In *In re Currency Conversion Fee*, plaintiff-cardholders challenged the disclosure and price of credit and debit card foreign transaction fees.[194] The class period extended from February 1, 1996 through, and including, November 8, 2006.[195] There was significant variability in damages for the class—some people had not been abroad at all, while others spent thousands of dollars abroad.[196] Any person who held an affected card issued in the United States as of November 8, 2006 was a member of the

192. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).

193. *Id.*

194. *In re* Currency Conversion Fee Antitrust Litig., 263 F.R.D. 110, 115 (S.D.N.Y. 2009).

195. Currency Antitrust Litig. Settlement Adm'r, Frequently Asked Questions (Aug. 31, 2016) (on file with author).

196. *Id.*

Settlement Injunctive Class.[197] Any person who made a foreign transaction on at least one of those cards between February 1, 1996 and November 8, 2006 was a member of the Settlement Damages Class.[198] "Only members of the Settlement Damages Class were allowed to seek refunds by submitting a claim."[199]

At the time the settlement was approved, a mechanism was set up for people to prove actual damages. All claimants received a minimum of twenty-five dollars by simply being a member of the damages class.[200] But if a plaintiff could prove higher damages, that plaintiff could prove actual damages. Plaintiffs could do this by opting to either provide their travel information, which would be entered into an algorithm to determine a refund amount, or provide the dollar amount of foreign transactions incurred on their cards during the claim period.[201] Because the combined preliminary payment amount for all authorized claimants was greater than the amount of available settlement funds, all authorized claimants received a pro rata distribution of the available settlement funds.[202] A payout structure similar to that in *In re Currency Conversion Fee* could be used in data breach actions to account for the variability plaintiffs are likely to experience in damages.

6. Practical Reality Precludes Compensation for Sorting-Things-Out Costs

Practically speaking, the cost of sorting things out is not a kind of injury that current doctrine is likely to recognize. While it is possible to see some tangible, identifiable loss in sorting-things-out costs, whether that is the kind of loss that warrants federal jurisdiction is dubious. There would be significant problems in recognizing standing for reasonable and substantial sorting-things-out costs, such as defining "substantial" and monetizing the costs. Additionally, compensatory and deterrent justifications for recognizing the cost of sorting things out as an injury fall short.

a. Difficulty in Calculating Sorting-Things-Out Costs

The difficulty associated with calculating sorting-things-out costs could potentially allow every data breach action to survive a motion to

197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.*
201. *Id.*
202. *Id.*

dismiss, which is all class action plaintiffs generally have to do to get a settlement payout as plaintiffs could simply allege substantial costs. While only compensating substantial sorting-things-out costs may not seem in line with the core purpose of class actions—to allow people with small claims to pursue a remedy—in fact, it is, and it is because of this that such compensation becomes impractical. Even *substantial* sorting-things-out costs amount to small monetary claims.

For example, in *Paytime*, even though the employee suffered a significant inconvenience in his increased commute, what concrete, monetary expense did he actually incur? The cost of gas? If people were having to take time off of work to sort things out after a breach, then perhaps that would constitute a substantial, easily calculable expense in the form of loss of earnings. However, that is unlikely the case. What is more likely is that sorting things out is a mere inconvenience for people, infringing on their television or leisure time. What should damages for lost television time be? In reality, substantial loss of time is unlikely to equate to a substantial loss of earnings. In all likelihood, plaintiffs claiming costs for sorting things out would largely be seeking compensation for mere annoyance, which the Court historically has not recognized as sufficient for Article III standing. This creates a significant challenge in calculating the rate at which time expended sorting things out should be reimbursed, such that it might preclude the Court from recognizing it as an injury.

Class actions are important when large amounts of people are out small amounts of money, but the reality of data breach cases is that the amount of money people are out is much smaller than the cost to distribute; so in the end, small losers are unable to be compensated.

b. Justifications for Compensating Sorting-Things-Out Costs Fall Short

When damages get sufficiently small, compensation becomes impractical, as illustrated above, and reasons for allowing class actions shift from compensatory to deterrent purposes. Here, companies are already sufficiently incentivized to avoid data breaches. For example, following Target's 2013 security breach, it paid $10 million in March 2015 to settle a federal class action customer lawsuit, $67 million in August 2015 to settle with Visa, and another $39 million in December 2015 to settle with several U.S. banks.[203] In addition, Target incurred $61 million in expenses in its 2013 fourth quarter from the breach ($44 million of which was paid by insurance), including: costs for data breach investigation, credit monitoring

203. Ahiza Garcia, *Target Settles for $39 Million over Data Breach*, CNN: MONEY (Dec. 2, 2015, 5:48 PM), http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/.

and identity theft protection services for customers, increased staffing in call centers, and legal expenses.[204] Overall, Target has faced "more than 80 related lawsuits, including . . . federal and state investigations into how the company responded to the attack."[205] Analysts estimated breach-related costs to be hundreds of millions of dollars.[206] "Concerns over the breach kept shoppers away during the crucial [2013] holiday season, leading to a 5.5% drop in the number of transactions, the largest quarterly decline since Target began reporting the statistic in 2008."[207] "[I]ts profit fell nearly 50% in its fourth fiscal quarter of 2013 and declined by more than a third for all of 2013."[208]

Following the Ashley Madison hack, Ashley Madison's parent company, recently rebranded as Ruby Corp.,[209] became the subject of a U.S. Federal Trade Commission investigation.[210] The breach cost Ruby Corp. more than a quarter of its revenue.[211] Ruby Corp. replaced its CEO and is spending millions to improve security.[212] It has been flooded with class action lawsuits—both in the United States and Canada.[213]

Costs like these, in addition to the risk data breaches pose to companies' internal information, comprise a significant deterrent. These realizations reduce the persuasiveness of compensatory and deterrent justifications for recognizing sorting-things-out costs as an injury in data breach cases.[214]

204. Maggie McGrath, *Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep on Coming*, FORBES (Feb. 26, 2014, 9:21 AM), www.forbes.com/sites/ maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#168d13c85e8c.

205. Paul Ziobro, *Target Earnings Slide 46% After Data Breach*, WALL ST. J. (Feb. 26, 2014, 6:36 PM), https://www.wsj.com/articles/SB10001424052702304255604579406694182132568.

206. *Id.*

207. *Id.*

208. McGrath, *supra* note 204.

209. Anne Steele, *Ashley Madison Parent Rebrands Itself as Ruby Corp.*, WALL ST. J. (July 12, 2016, 7:16 AM), http://www.wsj.com/articles/ashley-madison-parent-rebrands-itself-as-ruby-corp-1468322180.

210. Alastair Sharp & Allison Martell, *Infidelity Website Ashley Madison Facing FTC Probe, CEO Apologizes*, REUTERS (July 5, 2016, 4:01 PM), http://www.reuters.com/article/us-ashleymadison-cyber-idUSKCN0ZL09J.

211. *Id.*

212. Steele, *supra* note 209.

213. Sharp & Martell, *supra* note 210.

214. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 186 (2000) ("We recognize that there may be a point at which the deterrent effect of a claim for civil penalties becomes so insubstantial or so remote that it cannot support citizen standing.").

## IV. IMPACT OF PROPOSED STANDARD ON DATA BREACH CASES

Courts have generally treated increased risk of identity theft or fraud and expenses required to mitigate such risk, the most common theories of injury in data breach lawsuits, "as rising or falling with one another."[215] Courts have not recognized mitigation expenses as an injury without recognizing increased risk of identity theft or fraud. Recognizing injuries incurred in mitigating future harm but rejecting increased risk of future harm as an injury would pave the way for a new framework for establishing injury.

Setting a clear standard that rejects increased risk of identity theft or fraud as a cognizable injury would presumably reduce the number of data breach actions brought in federal court, as courts in the Sixth, Seventh, and Ninth Circuits have recognized increased risk of identity theft or fraud as an injury.[216] Under the proposed standard, a risk of future identity theft or fraud would never be sufficiently imminent because even if identity theft or fraud occurs, it must then be shown that any costs incurred were not remedied.

On the other hand, recognizing one year of monitoring services as a cognizable injury would likely have an insignificant effect because hacked companies typically already offer a complimentary year of monitoring services. However, even where monitoring services are provided, the purchase of monitoring services may still constitute an injury where the monitoring provided is not effective.[217] Further, while one year of monitoring is presumptively sufficient under this Note,[218] plaintiffs may be able to prove that longer monitoring is required.[219]

If the Court were inclined to recognize the cost of sorting things out as an injury, it would likely increase the number of data breach actions brought as courts have generally rejected these expenses as injuries. While

215. John L. Jacobus & Benjamin B. Watson, Clapper v. Amnesty International *and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 1, 17 (2014).

216. Galaria v. Nationwide Mut. Ins., 663 Fed. App'x 384, 388 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692, 696 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014).

217. *See* discussion *supra* Part III.B.4.

218. *See* discussion *supra* Part III.B.1.

219. *See Galaria*, 663 Fed. App'x at 388–89 (recognizing plaintiffs' expenditures on monitoring services as an injury where the risk of identity theft or fraud was continuing and the defendant only provided monitoring services for one year).

the Sixth Circuit has recognized these expenses in the absence of actual identity theft or fraud,[220] the Seventh Circuit has only recognized these expenses where actual identity theft or fraud occurred.[221] If the Court followed this Note's proposed way of recognizing sorting-things-out costs, it would recognize reasonable and substantial sorting-things-out costs as long as customers have been informed of a breach affecting their sensitive information and have no reason to believe that insufficient information was accessed for any real harm to come from the breach, regardless of whether any fraud has occurred.

In all of this, it is important to keep in mind that even if plaintiffs lack Article III standing, they may bring their action in state court, which is not subject to the same Article III standing constraints. Several federal courts have remanded data breach actions to state court where they had been removed to federal court and lacked Article III standing.[222]

## CONCLUSION

Going forward, hacking is projected to focus on personalized attacks, and pre-packaged cyber attacks are predicted to increase.[223] With today's technology, "our behavioral patterns are always being monitored."[224] Experts predict that attackers will take advantage of "this constant collection of personal data."[225] Cyber attacks as packaged goods are expected to increase in popularity, making "personal attacks accessible to those who do not necessarily have the skills or experience to launch attacks themselves," thus enabling neighbors, colleagues, friends, and family members to access another's personal data to engage in personal attacks.[226] This is expected to shift motives for cyber attacks from financial gain to "embarrassment, harassment and vandalism."[227]

We can already see this motive shift playing out with the Ashley

220. *Id.* at 388.

221. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016); *Remijas*, 794 F.3d at 694.

222. *See, e.g.*, Bradix v. Advance Stores Co., No. 16-4902, 2016 U.S. Dist. LEXIS 87368, at *13 (E.D. La. July 5, 2016); Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2016 U.S. Dist. LEXIS 66404, at *20–22 (D. Md. May 18, 2016) (citing Spokeo, Inc. v. Robins, 135 S. Ct. 1892 (2015)).

223. Mike Hickson, *Cyber Threats and Hacking Trends for 2016*, IT SEC. GURU (Nov. 26, 2015), http://www.itsecurityguru.org/2015/11/26/cyber-threats-and-hacking-trends-for-2016/.

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*

Madison breach, where "Impact Team" hackers initially attempted to blackmail Ruby Corp. (formerly Avid Life Media) with stolen information to get it to remove Ashley Madison's site and its sister site, Established Men.[228] In that hack, the goal of the hackers did not appear to be financial gain, but rather the hackers appeared to be taking a moral stance. After the hack, people whose information was released became individual targets of blackmail, harassment, and extortion.[229]

With such risk and uncertainty surrounding liability for data breaches, attention will likely turn to cyber risk insurance.[230] Cyber risk insurance is "one of the few commercial property/casualty insurance products bucking the trend toward stagnant or lower premium rates."[231] Carriers have been expanding cyber risk coverage, such that it has become more than just a standard insurance product: it has become "a product where risk management services are being offered to help protect companies against [] loss."[232] So far, there has been very little case law analyzing cyber risk under cyber risk policies. Most cyber risk cases have tried to find coverage under general liability or property policies.[233] It will likely take some time for case law on cyber risk policies to develop. So far, case law has not provided comfort to companies hoping to rely on their cyber risk policies to cover them in the event of a breach. In *Travelers Property Casualty Co. of America v. Federal Recovery Services, Inc.*, a Utah district court denied coverage where a cyber risk policy provided coverage for an errors and

228. Joseph D. McClendon, *Managing Cyberthreats After the Ashley Madison Breach*, LAW360 (Aug. 13, 2015, 1:14 PM), http://www.law360.com/articles/689694/managing-cyberthreats-after-the-ashley-madison-breach.

229. Dan Goodin, *Exposed Ashley Madison Members Targeted by Scammers and Extortionists*, ARS TECHNICA (Aug. 24, 2015, 1:55 PM), http://arstechnica.com/security/2015/08/exposed-ashley-madison-members-targeted-by-scammers-and-extortionists/; Sheelah Kolhatkar, *I Was Harassed After the Ashley Madison Hack*, BLOOMBERG (Aug. 24, 2015, 10:51 AM), http://www.bloomberg.com/news/articles/2015-08-24/i-was-harassed-after-the-ashley-madison-hack; *Police: Ashley Madison Hack Might Have Led to Suicides*, USA TODAY (Aug. 24, 2015, 3:38 PM), http://www.usatoday.com/story/news/nation-now/2015/08/24/police-ashley-madison-hack-extortion-crimes-suicides/32269699/; Catherine Townsend, *'It's A Modern Witch Hunt': Woman Reveals How Her Marriage and Career Were Almost Destroyed After She Was Falsely Accused of Being An Ashley Madison Adulterer*, DAILY MAIL (Aug. 25, 2015, 4:06 PM), http://www.dailymail.co.uk/femail/article-3210508/It-s-modern-witch-hunt-Woman-reveals-marriage-career-destroyed-falsely-accused-Ashley-Madison-adulterer.html.

230. *See, e.g.*, *Banks Rush to Buy Cyber Liability Insurance as Digital Payments Rise*, GADGETS360 (Feb. 13, 2017), http://gadgets.ndtv.com/internet/news/banks-rush-to-buy-cyber-liability-insurance-as-digital-payments-rise-1658864.

231. Stephanie K. Jones, *Cyber Insurance: An Evolutionary Coverage*, INS. J. (Dec. 21, 2015), http://www.insurancejournal.com/magazines/features/2015/12/21/391961.htm.

232. *Id.*

233. *See generally* Metro Brokers, Inc. v. Transp. Ins., 603 Fed. App'x 833, 835 (11th Cir. 2015) (analyzing property coverage); Eyeblaster, Inc. v. Fed. Ins., 613 F.3d 797, 801–03 (8th Cir. 2010) (analyzing general liability coverage).

omissions wrongful act, which was defined to include "any error, omission, or negligent act," and plaintiffs alleged "knowledge, willfulness, and malice."[234]

While eventually cyber risk insurance may provide some peace of mind for defendants (at a cost), monitoring may provide some peace of mind for plaintiffs, but plaintiffs cannot be certain that they will be reimbursed for the associated expenses. Standing has long been a point of contention in the judicial system; not every harm experienced can be compensated. At some point we have to take a step back, look at the big picture, and ask if resources spent on this kind of litigation are worth it. Is this something federal courts should be adjudicating? Ultimately, given the circumstances surrounding data breaches, most often it will not be. Nothing can provide absolute security when it comes to the cyber. There comes a point where victims' only option is to throw their hands in the air and shout "serenity now!"[235]

234. Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc., 103 F. Supp. 3d 1297, 1299, 1302 (D. Utah 2015).

235. *See Seinfeld: The Serenity Now* (NBC television broadcast Oct. 9, 1997).