Oklahoma Law Review

Volume 67 | Number 3

2015

Exposure Without Redress: A Proposed Remedial Tool for the Victimns Who Were Set Aside

Elizabeth T. Isaacs

Exposure Without Redress: A Proposed Remedial Tool for the Victimns Who Were Set Aside

Cover Page Footnote

Heartfelt thanks and acknowledgements go to the hard-working editorial team at the Oklahoma Law Review, to Professor Joseph Thai for his insight and support, and to my husband William Isaacs for serving as my sounding board as well as my partner.

COMMENTS

Exposure Without Redress: A Proposed Remedial Tool for the Victims Who Were Set Aside*

I. Introduction: Said the Joker to the Thief

When former CIA employee Edward Snowden drew back the curtain on the extent to which government security agencies gather information on the American people, it became a running joke that every e-mail and phone call is scrutinized by the National Security Agency (NSA) or other government officials. After law enforcement officers arrested a citizen who attempted to jump over the White House fence to spray paint a political message, late-night comedy host Jimmy Fallon joked, "If that guy really wanted to get a message to the President, he could have just written it in an e-mail to literally anyone."[1] Later, when the American citizenry expressed outrage over the extent of the NSA's domestic spying practices, political satirist Stephen Colbert responded, "Nation, the President has heard your calls for more oversight! In fact, he's heard all [of] your calls."[2]

Regardless of the comedic value of "Big Brother's" monitoring tactics, informational privacy is an important and highly personal concern for many people. Our desire for control over private information has increased despite a growing perspective that privacy is dead.[3] The private nature of our personal information may seem illusory in light of the myriad inevitable situations in which we surrender our personal information in exchange for common services. Applications for employment, mortgages, payroll direct deposit, and utilities like electricity and water all require the surrender of sensitive personal information as a matter of course.[4] In fact, employers

* Heartfelt thanks and acknowledgements go to the hard-working editorial team at the *Oklahoma Law Review*, to Professor Joseph Thai for his insight and support, and to my husband William Isaacs for serving as my sounding board as well as my partner.

1. *Late Night Political Humor*, POLITICAL IRONY, http://www.politicalirony.com/2013/06/22/late-night-political-humor-999/ (last visited Mar. 24, 2015). This quote was transcribed from a Late Night with Jimmy Fallon monologue, which was broadcast on NBC on Jun. 13, 2013.

2. *NSA Press Conference on Domestic Spying*, COLBERT REP., http://thecolbertreport.cc.com/videos/jngkv0/nsa-press-conference-on-domestic-spying (last visited Oct. 5, 2014).

3. *See* Alan Henry, *Why You Should Care About and Defend Your Privacy*, LIFEHACKER (Apr. 25, 2012), http://lifehacker.com/5904966/why-you-should-care-about-and-defend-your-privacy.

4. *See* Barbara Kiviat, *Guarding Your Social Security Number*, TIME (Dec. 4, 2007), http://content.time.com/time/business/article/0,8599,1690827,00.html.

need social security information to pay their employees, and banks are required to retain customers' social security numbers to comply with federal regulation.[5] So in some situations, giving out a social security number is unavoidable.

The inevitability of having to disclose private information does little to console the individual who receives a phone call or letter informing him that his private information may have leaked due to a data breach. That notification can precipitate a highly stressful and emotionally taxing time as the customer tries to regain control over his informational privacy.

An individual should address a data breach situation in three basic stages. The first step is to identify what type of information was subject to the breach.[6] An account number may allow an identity thief to make fraudulent charges on an existing account, which may not surface until the account-holder specifically reviews account activity.[7] But if the compromised information includes a social security number, the potential damage is even more insidious because a thief could open fraudulent accounts that are much harder to detect, which could lead to more out-of-pocket costs for the victim.[8]

Second, the customer must address potential compromise of existing accounts. The customer may monitor account activity closely for fraudulent transactions on financial statements, online, or by phone.[9] The customer may also cancel the existing account and open a new one with a different number.[10] Changing account numbers then creates more hassle by necessitating notification of other institutions that have authorization to withdraw automatically from the compromised account. Otherwise, they will not have the correct or updated account numbers from which to withdraw. When other institutions cannot withdraw funds, they may

5. KATHLEEN S. SWENDIMAN, CONG. RESEARCH SERV., RL3, THE SOCIAL SECURITY NUMBER: LEGAL DEVELOPMENTS AFFECTING ITS COLLECTION, DISCLOSURE, AND CONFIDENTIALITY 13-14 (2008), *available at* http://www.fas.org/sgp/crs/misc/RL30318.pdf (citing 31 C.F.R. 103.121(b)).

6. *Fact Sheet 17b: How to Deal with a Security Breach*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/how-to-deal-security-breach (last visited May 11, 2015) [hereinafter *How to Deal with a Security Breach*].

7. *Fact Sheet 17: Coping with Identity Theft: Reducing the Risk of Fraud*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/coping-identity-theft-reducing-risk-fraud (last visited Jan. 8, 2014).

8. Kiviat, *supra* note 4.

9. *How to Deal with a Security Breach*, *supra* note 6.

10. *Id.*

discontinue their services, assess fees, or report nonpayment to a credit bureau.

Third, the customer must address the risk of new fraudulent accounts appearing if the data breach exposed his personally identifying information, such as social security number and driver's license information.[11] He may choose to order and review copies of his credit report, hire a service to monitor his credit report, or do nothing on the hope that he will not find out that his account has been cleaned out the next time he tries to pay for dinner.[12]

Uncertainty fuels not only the difficulty in choosing a practical course of action, but also feelings of violation and helplessness. Sometimes notification of a data breach arrives with as little detail as "Your address and account number may have been compromised." The customer is left thinking, "How did the data breach happen? Did a group of criminal masterminds break the bank's encryption and steal the data in order to sell it to identity thieves? Did a disgruntled employee post a series of customer account snapshots on a random internet forum? Did a technologically savvy teenager decide he wanted to know where, when, and how often a bank's customers purchase liquor, gamble online, and buy medication? Or did someone neglect to shred a bag of paper that may be lost and will never be seen again?" Whether the vulnerable data is likely to be used immediately for identity theft is not the only concern. Compromised data could remain available and useful to identity thieves in perpetuity and may be distributed to any number of third parties because data is easy to replicate and distribute.

Customers have attempted to sue vendors that have experienced data breaches, basing their claims on theories of breach of implied contract, negligence, and negligent infliction of emotional distress, even before identity theft occurred.[13] Because plaintiffs bring these as class actions before the occurrence of fraudulent use of the breached data, the injuries alleged are, at most, increased risk of identity theft and emotional distress

11. *Id.*

12. *Id.*

13. *E.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632-33 (7th Cir. 2007); Reilly v. Ceridian Corp., No. 10-5142 (JLL), 2011 WL 735512, at *2 (D.N.J. Feb. 22, 2011), *aff'd*, 664 F.3d 38 (3rd Cir. 2011).

resulting from the defendant's failure to adequately protect the plaintiffs' data.[14]

The road to recovery of damages in a federal suit for increased risk of identity theft is littered with obstacles from beginning to end. Courts do not even agree on whether plaintiffs have standing to bring the action.[15] Article III, Section 2 of the U.S. Constitution creates standing in federal court. In this context, the analysis turns on whether an increase in risk of future harm constitutes sufficient injury-in-fact to confer Article III standing,[16] or whether they are merely "allegations of hypothetical, future injury[, which] do not establish standing under Article III."[17] There is currently a split among circuit courts about whether a plaintiff has standing to sue for increased risk of identity theft.[18] Although initial decisions in district courts did not recognize standing,[19] the Seventh and Ninth Circuits held that plaintiffs had standing based on similar rationales to other claims for future harm that currently recognize standing.[20] However, the Third Circuit has now created conflict with the other two courts with a well-reasoned but criticized opinion that denied standing.[21]

Even when courts recognize standing for suits alleging increased fraud risk, plaintiffs face obstacles in meeting prima facie elements of common law negligence and breach of implied contract because courts hold that increased fraud risk does not present a compensable injury.[22] Further analysis suggests that plaintiffs would have difficulties proving other prima facie elements such as actual and legal causation, and breach of standard of care.[23] Therefore, a plaintiff is unlikely to recover damages even if the suit survives a challenge to standing.

---

14. Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1369 (2013).

15. *Id.* at 1370.

16. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-42 (9th Cir. 2010) (citing Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (Toc), Inc., 528 U.S. 167, 180-81 (2000)).

17. Reilly v. Ceridian Corp., 664 F.3d 38, 41 (3d Cir. 2011).

18. *See infra* text at Part II.C.

19. *See infra* text at Part II.B.

20. *See infra* text at Part II.C.1.

21. *See infra* text at Part II.C.2.

22. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635-40 (7th Cir. 2007).

23. *See infra* text at Part III.

Some legal scholars have called for comprehensive legislation on protection of private data,[24] including (in some cases) establishment of a private right of action for claims based on increased fraud risk (Data Breach Claims).[25] Other scholars have proposed judicial recognition of increased fraud risk as sufficient to meet the "injury-in-fact" requirement for standing in federal courts.[26]

This Comment reviews obstacles to recovery in a Data Breach Claim in detail. Part II analyzes the circuit split regarding standing and explains how the Third Circuit's latest decision, which developed a test for standing in Data Breach Claims, is more consistent with established law. Part III discusses the inefficacy of common law causes of action as bases for Data Breach Claims because these cases lack key prima facie elements. Part IV compares proposed legislative solutions and creates a sketch for a private right of action. A statutory right to sue would provide effective redress to plaintiffs, and should take into consideration current obstacles in data breach litigation.

II. There's Too Much Confusion

A. A Basic Under-"standing"

Federal jurisdiction is limited to actual "cases or controversies."[27] In order to invoke federal jurisdiction, plaintiffs have the burden of establishing three essential elements.[28] The first element plaintiffs must show is that they have suffered an "injury in fact."[29] Over time, the Supreme Court has refined the definition of injury in fact to require three basic elements. An injury in fact is an invasion of a legally protected interest that is "(a) concrete and particularized, . . . and (b) actual or imminent, not conjectural or hypothetical."[30] Second, plaintiffs must

24. Patricia Cave, Comment, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 769 (2013); Lori Chiu, Comment, *Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World*, 14 SAN DIEGO INT'L L.J. 281, 283-84 (2013).

25. Cave, *supra* note 24, at 769.

26. Galbraith, *supra* note 14, at 1371-72.

27. U.S. CONST. art. III, § 2.

28. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992); Linda R.S. v. Richard D., 410 U.S. 614, 616-17 (1973).

29. *Defenders of Wildlife*, 504 U.S. at 560.

30. *Id.* (citations omitted) (internal quotation marks omitted) (summarizing requirements for an injury in fact as developed in Supreme Court cases over time).

demonstrate that the injury is "'fairly . . . trace[able] to the challenged action of the defendant and not . . . th[e] result [of] the independent action of some third party not before the court.'"[31] Third, plaintiffs must show it is "likely," and not "merely 'speculative,' that the injury will be redressed by a favorable decision."[32]

Legally protected interests, for purposes of determining injury in fact, may include common law rights (established by property, contract, and tort law), constitutional rights, and statutory rights created by Congress.[33] A statutory right may confer standing even if the plaintiff's injury would not have been judicially cognizable at common law.[34] However, this does not give Congress unlimited authority to create causes of action. Although Congress may define protected rights for individuals and expand Article III standing to protect those rights, it is improper for the legislature to reach beyond the limits of Article III to allow citizens to sue for general enforcement of laws without some particularized injury.[35]

For example, in *Federal Election Commission v. Akins*, the Supreme Court recognized a "right to information" created by statute that would not have existed absent the statute.[36] The plaintiffs alleged sufficiently particularized injury because they were unable to obtain specifically sought information.[37] In contrast, the Court held in *Lujan v. Defenders of Wildlife* that Congress could not create standing by including a statutory clause allowing any private individual to enjoin a government agency's violation of the Endangered Species Act.[38] The right to enforce the statute in *Defenders of Wildlife* protected the survival chances of endangered species, which did not cause an injury by directly harming any plaintiff.[39] Even

31. *Id.* (alteration in original) (citations omitted).

32. *Id.* at 561 (citations omitted) (internal quotation marks omitted).

33. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 69-72 (4th ed. 2011) [hereinafter CHEMERINSKY, CONSTITUTIONAL LAW].

34. Warth v. Seldin, 422 U.S. 490, 514 (1975).

35. CHEMERINSKY, CONSTITUTIONAL LAW, *supra* note 33, at 70-72 (comparing the Supreme Court's recognition of statutory basis for standing in *Trafficante v. Metro. Life Ins. Co.*, 409 U.S. 205, 211-12 (1972), to the Court's refusal to recognize a statutory basis for standing in *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 562-63 (1992)).

36. *Id.* at 72 (citing 524 U.S. 11, 21 (1998)).

37. *Id.*

38. *Id.* at 71 (citing *Defenders of Wildlife*, 504 U.S. at 562-63). In essence, a statute that allows a citizen to enforce a law that protects a public right, rather than an individual right, warps the constitutional role of the judicial branch. *Defenders of Wildlife*, 504 U.S. at 576-77.

39. 504 U.S. at 558-59, 562-63.

though some plaintiffs alleged that they had visited the animals' habitats in the past, they did not testify to any plans (beyond general possibility) to visit the habitats in the future.[40]

The same analysis likely applies in federal court even when that court is dealing with a state law that confers standing in state court. In *Hollingsworth v. Perry*, the Supreme Court recognized California's right to allow proponents to defend their challenged initiatives in state court, but still required satisfaction of Article III requirements to invoke federal jurisdiction.[41]

In establishing "injury in fact," the Supreme Court has held that assertions of "possible future injury" that are not "certainly impending" are too speculative to satisfy Article III requirements.[42] For example, in *City of Los Angeles v. Lyons*, the Court held that the plaintiff did not have standing to seek an injunction against police chokeholds even after a plaintiff allegedly suffered an illegal chokehold at the hands of arresting officers.[43] The plaintiff's alleged risk of future injury relied on speculation that he would later be stopped by police and subjected to an illegal choke.[44] In another case, *Diamond v. Charles*, a pediatrician sought to appeal a case that struck down his state's anti-abortion law.[45] The appellant-pediatrician alleged that failure to enforce the law would injure his professional practice by reducing the number of potential patients by the number of otherwise illegal abortions performed.[46] The Court held that the appellant lacked standing because his asserted interest was based on unadorned speculation that fetuses saved from abortion "would survive and then find their way as patients to [the appellant]."[47]

The second and third requirements for Article III standing require a causal relationship between the defendant's conduct and the plaintiff's injury, and a remedial relationship between the plaintiff's injury and the relief sought. The requirement of causation necessitates that the injury is not "highly indirect and [does not result] 'from the independent action of some third party not before the court.'"[48] Redressability requires that the

40. *Id.* at 562-64.
41. 133 S. Ct. 2652, 2667-68 (2013).
42. Whitmore v. Arkansas, 495 U.S. 149, 158 (1990).
43. 461 U.S. 95, 105 (1983).
44. *Id.*
45. 476 U.S. 54, 56-61 (1986).
46. *Id.* at 66.
47. *Id.*
48. Allen v. Wright, 468 U.S. 737, 757 (1984) (internal citation omitted), *abrogated by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1387-88 (2014).

prospective relief sought will remove the harm.[49] If the grant of the relief sought will not make a difference in the plaintiff's injury, then a judicial disposition is no more than an advisory opinion.[50]

The driving force behind standing doctrine is consideration of whether the case in question is appropriate to be determined by the judiciary or by other branches of the federal government.[51] In writing both for the Court[52] and in other legal scholarship,[53] Justice Antonin Scalia stated that standing restricts the jurisdiction of the court in the interest of separation of powers by preventing judicial intervention in other branches of government in the name of furthering majority interests.[54] In other words, standing doctrine should prevent judicial involvement when plaintiffs are attempting to further the general interests of a group of people, but plaintiffs themselves suffer no injury in fact.[55] In these cases, redress should come from the legislature or executive, which are designed to promote and enforce majority interests.[56]

In the case of a class action, the plaintiffs that represent the class must have standing derived from their own claims in order to seek relief.[57] The rationale behind this requirement is that in order to ensure rigorous advocacy on behalf of a party, the representative party must have a "'personal stake in the outcome.'"[58]

B. No Leg to Stand on in Federal District Courts

Initial cases against entities that experienced data breaches resulted in a variety of positions among the federal district courts.[59] A few district courts declined to recognize standing based on increased risk of identity theft.[60]

---

49. Warth v. Seldin, 422 U.S. 490, 505 (1975).

50. *See* CHEMERINSKY, CONSTITUTIONAL LAW, *supra* note 34, at 78-79.

51. *See Allen*, 468 U.S. at 752 ("[T]he law of Art. III standing is built on a single basic idea—the idea of separation of powers.").

52. Lujan v. Defenders of Wildlife, 504 U.S. 555, 559-60 (1992).

53. Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 894 (1983).

54. *See Defenders of Wildlife*, 504 U.S. at 559-60; Scalia, *supra* note 53, at 894-96.

55. *See Defenders of Wildlife*, 504 U.S. at 573-74.

56. *Id.* at 576-77.

57. O'Shea v. Littleton, 414 U.S. 488, 493-95 (1974).

58. *Id.* at 493-94 (citation omitted).

59. *See* Jay M. Zitter, Annotation, *Liability for Risk of Future Identity Theft*, 50 A.L.R.6th 33, 43-46 (2009).

60. *E.g.*, Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006) ("Because 'assertions of potential future injury do not satisfy the injury-in-fact test,' [p]laintiff's claims must be dismissed for lack of standing." (internal

Other district courts used similar reasoning, but found lacking prima facie elements (namely compensable injury) of the cases.[61] Although rulings on the merits may support an inference that these latter courts implicitly recognized standing, the issue of standing does not appear to have been argued and no opinions specifically find that a plaintiff had standing based on increased fraud risk.[62] Thus, the application of standing doctrine to data breach claims was largely unsettled and inconsistent before the federal appellate courts weighed in on the issue.

C. The So-Called Circuits' Standing Split

Federal appellate courts disagree on whether increased risk of identity theft is sufficient to support standing. The Seventh and Ninth Circuits recognize standing (contrary to the initial trend in lower courts).[63] The Third Circuit, however, has declined to recognize standing.[64] Although legal scholars interpret this as a circuit split,[65] the latest circuit decision may also be interpreted as having created a test to determine standing in light of pleaded facts that were insufficient to show that any harm actually occurred.

1. Initial Circuits Stand United

The Seventh and Ninth Circuits currently recognize standing for data breach suits as a result of decisions in 2007 and 2010, respectively. Both decisions rested on analogy to other valid claims for risk of future injury, such as toxic exposure and defective medical devices.[66]

---

citation omitted)); Key v. DSW Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) ("Because [p]laintiff has failed to allege that she suffered injury-in-fact that was either 'actual or imminent,' this Court is precluded from finding that she has standing under Article III.").

61. *E.g.*, Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) (granting summary judgment to defendant on claims of negligence and breach of contract because plaintiffs had "shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm"); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (dismissing complaint because "there [was] reason to believe that Michigan's highest court would reject a novel legal theory of damages which is based on a risk of injury at some indefinite time in the future").

62. *See* Zitter, *supra* note 59.

63. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (noting plaintiffs had standing to sue, even though the damages the plaintiffs sought were not compensable as a matter of law).

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

65. *E.g.*, Cave, *supra* note 24, at 773; Galbraith, *supra* note 14, at 1381-85.

66. *Krottner*, 628 F.3d at 1142; *Pisciotta*, 499 F.3d at 634 n.3.

a) Pisciotta v. Old National Bancorp *(Seventh Circuit)*

The Seventh Circuit recognized standing for increased fraud risk in *Pisciotta v. Old National Bancorp*—the first federal appeals case to do so.[67] In *Pisciotta*, the defendant-bank had collected personal data from consumers who applied for loans through the bank's website.[68] The personal data for each plaintiff-customer depended on the different applications submitted to the website, but overall, the data included names, addresses, social security numbers, dates of birth, driver's license numbers, and financial account information.[69] The data collected by Old National Bancorp was compromised after the bank's web hosting facility experienced a data breach that was characterized in a subsequent investigation as "sophisticated, intentional, and malicious."[70] The plaintiffs sued the bank on state common law theories of negligence and breach of implied contract.[71]

The Seventh Circuit noted that at the time, many district courts (including the trial court in *Pisciotta*) had held that they lacked subject-matter jurisdiction because plaintiffs had not yet suffered sufficient injury in fact to satisfy Article III standing requirements.[72] However, the Seventh Circuit reversed, citing cases from other circuit courts in which threat of future harm that resulted from exposure to toxic substances and use of defective medical devices satisfied standing requirements.[73] The *Pisciotta* court explained its decision through citations, in two footnotes, that referred to other types of cases involving threat of future harm.[74] The footnotes included no explanation of why standing was recognized in the cited cases and no analogy to data breaches beyond the fact that increased fraud risk is also threat of future harm.[75] With that being the extent of its standing analysis, the *Pisciotta* court turned to the merits of the action.[76]

Ultimately, the Seventh Circuit dismissed the cause of action for failure to meet prima facie elements of the common law claims.[77] The court

67. 499 F.3d at 633-34.
68. *Id.* at 631.
69. *Id.*
70. *Id.* at 632.
71. *Id.* at 633.
72. *Id.* at 634.
73. *Id.* at 634 nn.3-4.
74. *Id.*
75. *See id.*
76. *Id.* at 635-40.
77. *Id.* at 640.

declined to expand Indiana state law to recognize increased fraud risk as "compensable damages" sufficient for either negligence or breach of implied contract actions.[78] The plaintiffs sought compensation for credit-monitoring services resulting from the data breach.[79] The Seventh Circuit analyzed whether "the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing *compensable injury and consequent damages* to state a claim for negligence or for breach of contract."[80] The court reviewed three sources of guidance in its analysis: Indiana statutes, Indiana cases, and cases interpreting other states' laws.

First, the Seventh Circuit looked to Indiana state statutes.[81] After the defendant's data breach occurred, Indiana passed a data breach statute, which imposed an affirmative duty on private database owners to disclose a data breach to potentially affected consumers.[82] The statute did not create a duty to compensate individuals affected by the breach; nor did it create a private right of action for consumers to sue the database owner.[83] Because the sole remedies provided by the statute were state-enforced penalties, the court concluded that state legislation did not support recognition of credit-monitoring costs as compensable damages.[84]

Second, the Seventh Circuit reviewed Indiana cases involving comparable issues.[85] The closest analogy, found in cases for toxic tort liability, afforded no more support than given by state legislation.[86] The Supreme Court of Indiana's cases suggested that compensable injury occurs when a plaintiff could be reasonably diagnosed with actual illness or disease, rather than at the time of exposure to toxic substances.[87] In fact, Indiana case law indicated that medical-monitoring costs resulting from exposure to toxic substances were not recoverable.[88]

Third, the Seventh Circuit looked to case law interpreting other states' laws with respect to recovery of credit-monitoring costs.[89] After reviewing

78. *Id.* at 637, 639.
79. *Id.* at 632.
80. *Id.* at 635.
81. *Id.* at 636-37.
82. *Id.* at 636.
83. *Id.* at 637.
84. *Id.*
85. *Id.* at 637-39.
86. *Id.* at 638-39.
87. *Id.* at 639.
88. *Id.*
89. *Id.* at 639-40.

cases from Ohio, Minnesota, Arizona, and Michigan, the court concluded that state laws overwhelmingly do not recognize increased risk of identity theft alone as compensable injury.[90]

b) Krottner v. Starbucks Corp. *(Ninth Circuit)*

The Ninth Circuit employed a more rigorous analysis of standing doctrine in *Krottner v. Starbucks Corp.*[91] In this case, plaintiffs were then-current and former Starbucks employees whose unencrypted names, addresses, and social security numbers were contained in a laptop that was stolen from Starbucks.[92] The laptop contained the personal data of approximately 97,000 employees.[93] Twenty days after the breach, Starbucks sent a letter to all affected employees to notify them of the breach and offer a year of free credit-monitoring services through Equifax.[94] Despite receipt of these services, the plaintiffs alleged that they still spent "substantial amounts of time" monitoring for fraudulent activity and suffered anxiety and stress as a result of the data breach.[95] The plaintiffs sued on grounds of negligence and breach of implied contract.[96]

Notably, the Ninth Circuit did not address whether a data breach claim satisfies the second and third requirements for standing because those requirements were undisputed before the district court.[97] However, because standing is determinative of whether there is proper subject-matter jurisdiction, the Ninth Circuit was still under an independent duty to discuss the second and third requirements sua sponte if they presented barriers to standing.[98]

The Ninth Circuit separately analyzed whether emotional distress and increased fraud risk could be sufficient injury in fact to confer standing. As a present injury, one plaintiff's allegation of "generalized anxiety and stress" was sufficient to confer standing, but only as to that plaintiff.[99] The Ninth Circuit referred to its own decisional history regarding future injury,

90. *Id.*
91. 628 F.3d 1139, 1141-43 (9th Cir. 2010).
92. *Id.* at 1140.
93. *Id.*
94. *Id.* at 1140-41.
95. *Id.* at 1141.
96. *Id.*
97. *Id.*
98. *See id.* ("We have an independent obligation to examine standing to determine whether it comports with the case or controversy requirement of Article III, Section 2 of the Constitution.").
99. *Id.* at 1141-42.

in which it had previously held that "the possibility of future injury may be sufficient to confer standing on plaintiffs; threatened injury constitutes 'injury in fact.'"[100] However, the threatened future injury must pose an "*immediate*" danger of "*direct* injury," and not be conjectural or hypothetical in order to constitute injury in fact.[101]

Like the Seventh Circuit in *Pisciotta*, the Ninth Circuit analogized increased risk of identity theft to suits arising from exposure to toxic substances and from harm to the environment.[102] Plaintiffs in need of medical monitoring services satisfied requirements for injury in fact, and environmental claims asserting threatened future injury sufficiently established injury in fact.[103] The Ninth Circuit held that the increased risk of identity theft was not too hypothetical or conjectural in light of the facts; the criminal element in the theft of the laptop made the risk of identity theft a "credible threat of real and immediate harm."[104] Had the suit been brought before the laptop was stolen on the theory that the possible future theft of the laptop created an increased risk of identity theft, the court stated the injury would then be too speculative and conjectural.[105] Thus, the Ninth Circuit may have based its decision on the fact that a criminal act had already been perpetrated by a third party that lends itself to the inference that identity theft is likely to result.

Even after deciding that increased fraud risk is sufficient to confer standing, however, the Ninth Circuit issued a separate memorandum opinion dismissing the plaintiffs' claim of negligence due to a lack of compensable injury, and dismissing the plaintiffs' claim of breach of implied contract due to separate factual grounds.[106] Regarding the issue of compensable injury, the Ninth Circuit quoted Washington case law: "The mere danger of future harm, unaccompanied by present damage, will not support a negligence action."[107] The Ninth Circuit concluded that the plaintiff's injuries originated from the risk of future harm, and thus were not recoverable.[108]

---

100. *Id.* at 1142 (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 947 (9th Cir. 2002)).

101. *Id.* (quoting Scott v. Pasadena Unified Sch. Dist., 306 F.3d 646, 656 (9th Cir. 2002)).

102. *Id.*

103. *Id.*

104. *Id.* at 1143.

105. *Id.*

106. Krottner v. Starbucks Corp., 406 F. App'x 129, 131-32 (9th Cir. 2010).

107. *Id.* at 131 (quoting Gazija v. Nicholas Jerns Co., 543 P.2d 338, 341 (Wash. 1975)).

108. *Id.*

Until the emergence of the Third Circuit's opinion on standing, the only other indication of disagreement was dicta from the Sixth Circuit. The Sixth Circuit had recognized standing for actual financial harm resulting from fraudulent conduct, but had indicated that mere increased risk of identity theft in the future was "somewhat 'hypothetical' and 'conjectural.'"[109] However, until the Third Circuit's decision in *Reilly v. Ceridian Corp.*,[110] the only circuit courts to rule on standing for increased risk of identity theft held that the plaintiffs had standing.

2. The Third Circuit Stands Alone

The court in *Reilly* based its opinion in part on a standard developed from its own prior decisions—that prospective damages are too conjectural when the asserted injury cannot be described "without beginning the explanation with the word 'if.'"[111] This standard is a plain-language way of explaining that threat of future harm cannot constitute injury in fact when that threat is predicated on a malicious act of a third party, and there is no evidence that the act is likely to occur.[112]

Interestingly, the Third Circuit asserted that *Pisciotta* and *Krottner* were inapposite because those cases involved conduct by potential identity thieves that more convincingly indicated that they were trying to use the stolen data for fraudulent purposes.[113] For example, the Third Circuit noted that in *Pisciotta*, the data breach was "sophisticated, intentional, and malicious" and resulted in actual unsuccessful attempts to open fraudulent accounts.[114] The Third Circuit characterized other circuits' analogy of increased fraud risk to defective-medical-device, toxic-substance-exposure, and environmental-injury cases as "skimpy rationale" because the analogy ignored basic elements of standing such as imminence of injury.[115] Consistent with the test that requires injuries to be explainable without beginning with the word "if," the Third Circuit distinguished data breach cases because in the other three types of cases, the damage has already occurred and has yet to manifest itself over time.[116] In the case of a data

109. *Krottner*, 628 F.3d at 1143 (discussing Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008)).
110. 664 F.3d 38 (2011).
111. *Id.* at 43.
112. *See id.*
113. *Id.* at 43-44.
114. *Id.*
115. *Id.* at 44.
116. *Id.* at 45.

breach, the plaintiffs must wait and see if some hypothetical third party would in fact inflict the damage.

The Third Circuit also distinguished the type of injury in terms of social importance. In cases involving defective medical devices and exposure to toxic substances, the injury alleged is human suffering or premature death.[117] The rationale behind recognizing this type of prospective risk of injury is that "[w]aiting for a plaintiff to suffer physical injury before allowing any redress whatsoever is both overly harsh and economically inefficient."[118] In environmental injury cases, the Third Circuit characterized the injury as one that is not remediable by monetary compensation.[119] The Third Circuit drew a sharp contrast between protecting natural resources and endangered species, which cannot be done through monetary compensation, and restoring victims of data breach, which is a monetary solution to an essentially monetary problem.[120] The opinion did not acknowledge increased risk of identity theft as an injury to one's very identity. It did not explain how the inadequacy of monetary damages as a remedy supports recognition of standing rather than cuts against the requirement that an injury be redressable.

The Third Circuit did not close the door completely on granting standing for increased risk of identity theft. In dictum, the court stated that the plaintiffs would sustain sufficient injury if they could show that the party that committed the data breach: "(1) read, copied, and understood [the plaintiffs'] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [plaintiffs'] names."[121]

The three criteria indicate that different facts involving the same central issue of increased risk of identity theft could be the basis of a proper action because if the criteria are met, then standing doctrine may be satisfied with respect to causation and redressability. By pleading facts that make it more likely that the ultimate harm—identity theft—will occur by fraudulent use of data obtained from the defendant's data breach, a plaintiff is more likely to show that the increased risk of identity theft is both "fairly traceable to the challenged actions of the defendant,"[122] and less speculative.

---

117. *Id.*
118. *Id.* (quoting Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 575 (6th Cir. 2005)).
119. *Id.*
120. *Id.* at 45-46.
121. *Id.* at 42.
122. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (alteration in original).

The requirements in *Reilly* seem to set a high bar because a plaintiff might only be able to plead sufficient facts to show that the requirements have been met if the plaintiff is the victim of a failed attempt at identity theft. Because the requirements focus on the intent and ability of the potential thief and do not specifically require a failed attempt on the individual plaintiff's identity, however, this may confer standing on an entire class of plaintiffs if there is a failed attempt on only one plaintiff who is not the designated representative.[123]

The *Reilly* requirements also seem to address the third Article III standing requirement of redressability because showing an indication of a potential identity thief's intent reduces the speculative nature of the injury. But how do the requirements make it any more likely that the requested relief (damages) is likely to remedy the harm of increased risk of identity theft? The plaintiffs may also have to show that the credit-monitoring services for which they seek reimbursement were actually effective in detecting or stopping the attempted fraud.

The legal community's response to the *Reilly* decision has been mixed. Although the *Reilly* court applied standing doctrine with more rigor than any other circuit court, legal scholars criticize it for "creat[ing] an unreasonable barrier for injured plaintiffs to reach the merits of their cases,"[124] and turning plaintiffs "away at the courthouse steps."[125] It creates a barrier to consumers seeking redress for their grievances and exposes the decision to criticism that often follows dispositions based on standing—that courts use standing as over-technical alternatives to deciding cases on the merits.[126] However, the holding in *Reilly* is more consistent with recognized standing jurisprudence and "serves the guiding twin rationales behind the doctrine: separation of powers and judicial efficiency."[127] More recently, scholars have begun to recognize that *the Third Circuit* did not explicitly break from the Seventh and Ninth Circuits, but distinguished the facts in

123. *See infra* Part IV.B.1.

124. Galbraith, *supra* note 14, at 1365.

125. *Id.* at 1385.

126. *See* Cave, *supra* note 24, at 787, n.149 (citing LISA A. KLOPPENBERG, PLAYING IT SAFE: HOW THE SUPREME COURT SIDESTEPS HARD CASES AND STUNTS THE DEVELOPMENT OF LAW 39-42 (2001); Gene R. Nichol, Jr., *Abusing Standing: A Comment on* Allen v. Wright, 133 U. PA. L. REV. 635, 636-37 (1985); Mark V. Tushnet, *The New Law of Standing: A Plea for Abandonment*, 62 CORNELL L. REV. 663, 664 (1977)).

127. *Id.* at 786-87.

Reilly from those of *Pisciotta* and *Krottner*.[128] Although the *Reilly* court criticized the analytical bases of the other two decisions, the three-prong test for standing produces consistent results when applied to the facts in those cases.[129]

D. The Reilly *Test: Stand and Deliver*

Because some fraud risk claims demand redress while others are too speculative, the higher standard created by the Third Circuit provides a compromise that recognizes potential injury in fact, but excludes the more dubious cases. The following analysis of standing doctrine shows why.

Injury must be a violation of a legally protected interest that is "actual or imminent, not conjectural or hypothetical" to be sufficient for constitutional standing.[130] Increased risk of identity theft is a risk of a future violation of a legally protected interest—an interest in not having one's identity stolen or suffering resultant financial loss or reputational harm vis-à-vis negative credit reporting.[131] The increased risk itself, however, is not a violation of a legally protected interest; the interest is at most one of not being at higher risk of becoming a victim of a crime. Even if the risk of future injury in fact is implicated, the future injury cannot be characterized as "imminent" because its occurrence depends on an intentional crime that may not happen at all, let alone "imminently."

The injury-in-fact requirement for constitutional standing "is qualitative, not quantitative, in nature," and the attendant "analysis is highly case-specific."[132] A qualitative evaluation of the nature and probability of the harm is pertinent to whether a court should confer standing.[133] Some circuits require a plaintiff to show that there is a "credible threat of harm" to

128. *E.g.*, John L. Jacobus & Benjamin B. Watson, Clapper v. Amnesty International *and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 3, ¶¶ 39-40 (2014), http://jolt.richmond.edu/v21i1/article3.pdf.

129. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011), *with* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140-42 (9th Cir. 2010), *and* Pisciotta v. Old Nat. Bankcorp, 499 F.3d 629, 631-32, 634 (7th Cir. 2007).

130. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (internal quotations marks omitted).

131. *See Identity Theft and Financial Fraud*, OFFICE FOR VICTIMS OF CRIME, U.S. DEP'T OF JUSTICE, http://www.ojp.usdoj.gov/ovc/pubs/ID_theft/idtheftlaws.html (last visited Oct. 22, 2013) (describing identity theft prosecution prior to 1998 as accomplished under "'false personation' statutes").

132. Baur v. Veneman, 352 F.3d 625, 637 (2d Cir. 2003).

133. *See id.*

establish standing because claims for increased risk of harm are "nebulous" and "potentially expansive."[134]

1. Analogies to Other Claims of Future Harm Do Not With-Stand Scrutiny

In recognizing that increased risk of identity theft is an injury in fact, the Seventh and Ninth Circuits analogize increased risk of identity theft to cases involving exposure to toxic substances, defective medical devices, and environmental harm.[135] But analogies to actions for risk of future bodily harm and future environmental harm are inapt for various reasons that become apparent on closer inspection of the rationale behind recognition of standing for these other claims.

a) Claims for Medical Monitoring Costs

In medical-monitoring claims (encompassing injuries arising from both toxic-substance exposure and defective medical devices), the purpose of medical monitoring is to detect symptoms of harm resulting from an injury that has already occurred.[136] Bodily injury occurs when a defective medical device is implanted and medical monitoring is required "to detect the onset of physical harm."[137] Similarly, when a person is exposed to a toxic substance, the "exposure itself causes an injury,"[138] and medical monitoring is used to detect the manifestation of symptoms of the injury that was caused by the exposure.[139]

In contrast to medical monitoring, credit monitoring does not detect symptoms of a harm that has already been initiated. Credit-monitoring

134. *Id.* (cautioning against broad application of its holding to recognize standing for increased risk of sickness resulting from ingestion of contaminated livestock); *see* Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002).

135. Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

136. Bouldry v. C.R. Bard, Inc., 909 F. Supp. 2d 1371, 1376 (S.D. Fla. 2012).

137. *Id.* (quoting Wyeth, Inc. v. Gottlieb, 930 So. 2d 635, 640 (Fla. Dist. Ct. App. 2006)) (internal quotation marks omitted).

138. Rhodes v. E.I. du Pont de Nemours and Co., 657 F. Supp. 2d 751, 759 (S.D. W. Va. 2009) (internal quotation marks omitted) (citing Sutton v. St. Jude Med., Inc., 292 F. Supp. 2d 1005, 1008 n.3 (W.D. Tenn. 2003)).

139. Metro-N. Commuter R.R. Co. v. Buckley, 521 U.S. 424, 449 (1997) (recognizing that medical monitoring is "necessary given the latent nature of many diseases caused by exposure to hazardous materials").

services are used to detect fraudulent activity,[140] which is itself a harm but not a symptom of a previous injury. Fraud does not always manifest after a data breach, and not all fraud results from data breaches. Identity theft is not a consequence of data breach, but of fraud. Data breach is just one of many ways in which an identity thief can obtain personal information, including mail theft, phishing, and spyware.[141] Moreover, data breach itself does not result in identity theft unless someone (not necessarily the data holder) intentionally and fraudulently uses the compromised data.[142]

In addition to the logical distinction between medical-monitoring claims and Data Breach Claims, there exists a compelling policy distinction in the ultimate injury that was expressed by the court in *Reilly*.[143] To force a plaintiff to suffer the physical manifestations of bodily injury or even premature death before being able to bring suit is "harsh and economically inefficient."[144] Premature death is not remediable. Some diseases resulting from toxic-substance exposure are incurable.[145] Defective medical devices can result in "painful, sometimes life-altering effects" for patients.[146] Data breaches, on the other hand, create only a risk of financial harm. Although financial harm resulting from actual fraud may be great, a financial damages award can reverse the harm. [147] Financial institutions generally compensate victims of identity fraud who experience direct financial losses.[148] Individuals who experience fraudulent activity on already-existing accounts generally receive expedient compensation from their own institutions with minimum effort required on the part of the victim.[149]

---

140. *See Fact Sheet 33: Identity Theft Monitoring Services*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/fs/fs33-CreditMonitoring.htm (last visited Oct. 18, 2013).

141. *What Is Identity Theft, and How Does It Happen?* TRUSTEDID, https://www.trustedid.com/types-of-identity-theft (last visited Oct. 18, 2013).

142. *See How to Deal with a Security Breach*, *supra* note 6 ("A security breach does not necessarily mean that you will become a victim of identity theft.").

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

144. *Id.* (quoting Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 575 (6th Cir. 2005)).

145. *E.g.*, *Asbestosis*, ASBESTOS.COM, http://www.asbestos.com/asbestosis (last visited Oct. 19, 2013) (explaining that asbestosis, which is a disease caused by inhalation of asbestos, has no known cure).

146. *See Defective Medical Devices*, DRUGWATCH, http://www.drugwatch.com/medical-devices (last visited Oct. 19, 2013).

147. *See* Rod J. Rosenstein & Tamera Fine, *Identity Theft: Coordination Can Defeat the Modern-Day "King" and "Duke*," U.S. DEP'T OF JUSTICE, http://www.justice.gov/usao/briefing_room/fin/id_theft.html (last visited Oct. 19, 2013).

148. *Id.*

149. *Id.*

However, identity theft may result in harms other than direct financial loss. For example, a criminal may use someone else's identity when interacting with law enforcement, which may result in a false entry in the fraud victim's criminal history or even an outstanding warrant.[150] Even in these cases, however, the harm is remediable—albeit in ways that place the burden on the victim.[151]

Medical monitoring also differs from credit monitoring as a preventive measure in key aspects. When specific conduct (e.g., toxic-substance exposure, implantation of a defective medical device, or even a car accident resulting in a possible head injury) necessitates particular medical diagnostic measures, the cost is "neither inconsequential nor of a kind the community generally accepts as part of the wear and tear of daily life."[152] Yet the monetary cost of medical monitoring can mitigate or prevent irreversible damages. For example, exposure to asbestos may increase chances of suffering from lung cancer.[153] Early detection of lung cancer through medical monitoring can allow a patient to start treatment early and perhaps even lower the risk of dying from the disease.[154] Even if credit monitoring lowers the risk or the severity of damages arising from fraud or identity theft, those damages, unlike death, are completely remediable by a monetary damage award. Thus, although some courts may be willing to recognize standing in medical-monitoring cases, there is a compelling policy reason for the expansion of standing in these cases that doesn't exist in credit monitoring cases: without medical monitoring, people could die sooner than with medical monitoring.

Suits that involve conduct contributing to environmental harm, like medical-monitoring suits, do not depend on an intentional criminal act of a third party to bring about the threatened injury. Although in some environmental-harm cases, plaintiffs seek injunctions to prevent continued

150. *Fact Sheet 17g: Criminal Identity Theft: What to Do if It Happens to You*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/criminal-identity-theft-what-to-do-if-it-happens-to-you (last visited May 11, 2015).

151. *Id.*

152. Friends for All Children, Inc. v. Lockheed Aircraft Corp., 746 F.2d 816, 825 (D.C. Cir. 1984).

153. 29 C.F.R. § 1910.1001 app. H (2014) ("[S]tudies have shown a definite association between exposure to asbestos and an increased incidence of lung cancer . . . .").

154. *Lung Cancer Prevention and Early Detection*, AM. CANCER SOC'Y, http://www.cancer.org/cancer/lungcancer-non-smallcell/moreinformation/lungcancerpreventionandearlydetection/lung-cancer-ped-toc (last visited Mar. 15, 2015).

unlawful conduct,[155] the conduct sought to be enjoined is the direct cause of threatened injury.[156] In data breach cases, however, the conduct of the defendant (failing to prevent a data breach) may increase the risk of future identity theft, but cannot, on its own, cause the identity theft. Further, the threatened harm of identity fraud is not necessarily associated with a higher likelihood that the *defendant* will commit identity theft, but that some third party might.[157]

b) Claims of Environmental Harm

Courts also recognized standing for fraud risk based on analogy to claims for environmental harm.[158] Just as in medical-monitoring cases, this analogy improperly compares causal relationships in environmental-harm suits with causal relationships in Data Breach Claims. Plaintiffs in environmental harm suits object to conduct that causes environmental harm directly—not conduct that causes environmental harm in conjunction with conduct of an independent third party.[159]

Moreover, the nature of the injury in fact differs between environmental-harm suits and Data Breach Claims. The violated interest or right in environmental-harm suits is the judicially recognized interest of a plaintiff to enjoy "the aesthetic and recreational values" of an affected environment.[160] If the threatened environmental harm occurs and results in permanent destruction of an endangered species[161] or streams and forests, then the violated interest may never recover.[162] For example, no amount of

155. *See, e.g.*, Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 173 (2000) (discussing citizen suit for injunctive relief to compel defendants to comply with the Clean Water Act).

156. *See, e.g.*, *id.* at 175-76, 181-82 (describing plaintiffs' injuries as arising from defendant's discharge of unacceptably high levels of mercury into a waterway).

157. *See How to Deal with a Security Breach*, *supra* note 6 (describing data breach scenarios in which sensitive information is obtained by third parties, such as third-party hacking, theft by third parties, and sale to third parties).

158. Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 n.3 (7th Cir. 2007).

159. *See, e.g.*, *Friends of the Earth, Inc.*, 528 U.S. at 175-77.

160. *Id.* at 183 (quoting Sierra Club v. Morton, 405 U.S. 727, 735 (1972)).

161. *See* Sierra Club v. U.S. Army Corps of Eng'rs, 645 F.3d 978, 995-96 (8th Cir. 2011).

162. Ohio Valley Envtl. Coal. v. U.S. Army Corps of Eng'rs, 528 F. Supp. 2d 625, 631-32 (2007) (explaining that permanent harm to streams and forests could occur due to defendant's plan to fill valleys during mining operations).

money can ever resurrect extinct species like the Tecopa Pupfish.[163] Identity theft, however, is remediable by monetary compensation of direct financial loss and correction of credit reports or criminal records.[164]

Environmental-harm suits also have a stronger basis for standing than data breach suits in the current legal environment because there are specific citizen-suit provisions in statutes like the Clean Air Act[165] and the Clean Water Act.[166] As discussed in subsection A of Part II of this comment, statutory creation of a legal right and a concomitant cause of action can form a sufficient basis for standing if the plaintiffs can also show a particularized injury.

2. Pisciotta *and* Krottner *Still Stand Under the* Reilly *Test*

The Third Circuit's dictum in *Reilly* leaves room for distinction from the facts in *Pisciotta* and *Krottner* rather than complete rejection of those decisions. The Reilly standard allows for recognition of standing if the perpetrator of the data breach "(1) read, copied, and understood [the plaintiffs'] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [plaintiffs'] names."[167] The standard restricts standing to claims that more likely include injury that is not just speculative because it applies to a category of claims in which data is actually compromised. Although the injury still depends on a third party's successful fraud attempt, the likelihood of the attempt and of its success is higher when the *Reilly* standard is met.

When the standard in *Reilly's* dictum is applied to facts from *Pisciotta* and *Krottner*, the results may still be confusing and dissatisfying. In *Pisciotta*, the data breach occurred when a hacker gained unauthorized access to the systems of the defendant's hosting facility.[168] The ensuing investigation of the data breach described the intrusion as "sophisticated,

163. Jill Harness, *7 Animals Humans Brought to Extinction*, NEATORAMA (Feb. 2, 2011), http://www.neatorama.com/2011/02/02/7-animals-humans-brought-to-extinction/#!lYd2D (explaining the demise of the Tecopa Pupfish as caused by the canalization of hot springs into bath houses in the Mojave Desert).

164. *See supra* Part III.1.a (noting harm incurred in identity theft is different from harm incurred in medical monitoring claims due to its compensable nature).

165. 42 U.S.C. § 7604 (2012).

166. 33 U.S.C. § 1365 (2012).

167. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

168. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).

intentional and malicious."[169] The Third Circuit stressed the finding of the investigative report from *Pisciotta* as a basis of *Pisciotta*'s lesser persuasive value.[170] The description from the report may make it seem more likely that the hacker "read, copied, and understood"[171] the personal information accessed because the intrusion was "sophisticated."[172] It may have been more likely that the hacker "intend[ed] to commit future criminal acts by misusing the information"[173] because the intrusion was "intentional and malicious."[174] And because the intrusion was "sophisticated, intentional and malicious,"[175] it is more likely that the hacker was "able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [the plaintiffs'] names."[176]

However, there is no mention in the opinion or briefing for *Pisciotta* of any actual attempt, failed or successful, of identity theft. The full results of the investigation were filed under seal, and the opinion gave no explanation of the basis of the characterization of the intrusion as "sophisticated, intentional and malicious" or the manner in which the description was used.[177] A sophisticated, intentional and malicious attack could have been aimed at the hosting facility system or at the data of any of the hosting facility's other customers. The further question remains unanswered: if the attack was so malicious and sophisticated as to render actual attempts at identity theft likely, why did no attempt occur between the dates of the attack in 2005[178] and the argument in the appellate court in 2007?[179] The description of the intrusion (sophisticated, intentional, and malicious) does not specifically indicate that the intruder read, copied, and understood the specific information at issue.

Application of the Third Circuit's standard to the facts in *Krottner* makes the injury appear much more likely because one of the plaintiffs received a warning one month after receiving notification of the data breach that "someone had attempted to open a new account using [the plaintiff's] social

169. *Id.*
170. *Reilly*, 664 F.3d at 44.
171. *Id.* at 42.
172. *Pisciotta*, 499 F.3d at 632.
173. *Reilly*, 664 F.3d at 42.
174. *Pisciotta*, 499 F.3d at 632.
175. *Id.*
176. *Reilly*, 664 F.3d at 42.
177. *Pisciotta*, 499 F.3d at 632.
178. *Id.*
179. *See* Transcript of Oral Argument, Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011) (No. 06-3817), 2007 WL 5514190, at *2.

security number."[180] Even if the failed attempt had not occurred, other facts provided sufficient bases to argue that because the data breach resulted from the theft of a laptop that housed "unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees,"[181] the hacker had likely "read, copied, and understood [the plaintiffs'] . . . information; . . . [intended] to commit future criminal acts by misusing the information; and . . . [was] able to use such information to the detriment of [the plaintiffs]" by attempting to steal their identities.[182]

However, *Krottner* poses another problem with redressability. When Starbucks notified its employees of the data breach, it offered credit-watch services through Equifax for one year.[183] The plaintiffs alleged that they had enrolled in the credit-watch services offered by Starbucks, but would continue incurring costs for credit monitoring after the expiration of the free services, and that despite the use of the credit-watch services plaintiffs still expended substantial amounts of time on personally monitoring their accounts and experienced generalized anxiety.[184]

The position of the *Krottner* plaintiffs raises two concerns. First, if increased risk of identity theft is sufficient as an injury in fact, how long does a person suffer that injury? If private data is posted on the internet and downloaded a thousand times, each person who downloaded it could retain hard copies of the information for decades; does that create an injury that requires decades of credit monitoring to redress? Second, if plaintiffs suffered injury (time spent monitoring accounts and generalized emotional distress) despite their use of credit-watch services, then an award of damages is probably insufficient to redress the plaintiffs' injury. Notably, the defendant in *Reilly* stated in its trial briefing that the plaintiffs "[did] not indicate whether they enrolled in the free credit monitoring and identity theft protection program offered by Ceridian through Equifax. They [merely] allege[d] that the program offered by Ceridian was 'inadequate.'"[185]

180. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010).

181. *Id.* at 1140.

182. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

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

184. *Id.*

185. Defendant Ceridian Corporation's Memorandum of Law in Support of Its Motion to Dismiss Plaintiffs' Complaint at 6, Reilly v. Ceridian Corp., 10-cv-05142 (D.N.J. Dec. 15, 2010), 2010 WL 9502109.

A court creates a "[d]etriment to [c]onsumers" by not recognizing standing[186] and even risks "unjustly limiting plaintiffs' access to the court."[187] But critics should consider the fact that data breach suits have consistently failed when asserted on traditional common law causes of action, even when standing is recognized, because increased risk of identity theft does not constitute a compensable injury.[188] If a court chooses to recognize standing but not compensable injury on the basis of increased risk of identity theft, then all the court has accomplished is granting plaintiffs the opportunity to go through additional (and costly) legal maneuvering, limited discovery, and even appellate proceedings, only to lose on summary judgment or dismissal.[189] Even if recognition of standing serves to increase the settlement value of a claim,[190] the cost of pre-trial litigation and small chance of success on the merits may outweigh the probable increase in value.

Thus, it is clear that the expansion of standing doctrine to include cases of increased risk of identity theft is not only inappropriate, but practically ineffective in providing plaintiffs with a satisfactory means of redress.

III. I Can't Get No Relief

Even if courts recognize standing, plaintiffs still face obstacles in establishing prima facie elements of common law claims. An understanding of the merits of a Data Breach Claim in the context of the common law causes of actions that plaintiffs typically allege is instructive in the development of a practical solution. In most cases, courts deny recovery because the causes of action pursued (i.e. negligence, breach of implied contract, and infliction of emotional distress) require a showing of compensable injury, which neither increased risk of identity theft nor the

186. Cave, *supra* note 24, at 786.

187. Galbraith, *supra* note 14, at 1386-87.

188. *See generally* Zitter, *supra* note 59.

189. *See, e.g.*, Krottner v. Starbucks Corp., 406 F. App'x 129, 131-32 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639-40 (7th Cir. 2007).

190. *See* Edward Brunet, Essay, *The Efficiency of Summary Judgment*, 43 LOY. U. CHI. L.J. 689, 689 (2012) ("[T]he settlement value of a case increases when a motion for summary judgment is denied."). Because standing is a threshold issue, early challenges to standing may allow defendants to avoid some costs, such as discovery. If the court rejects summary disposition, however, the risk of going to trial increases which may increase the value at which a defendant is willing to settle the claim. *See* 2 COMMERCIAL LITIGATION IN NEW YORK STATE COURTS § 5:38 (N.Y. Practice Series, Robert L. Haig et al. eds., 3d ed. 2013).

cost of credit-monitoring services sufficiently establish.[191] Aside from issues of damages, however, other pitfalls may cause a data breach claim to fail just as easily. For example, there may be difficulties in establishing causation if a plaintiff has experienced any data breaches in the past because a plaintiff may have to show that the identity theft, which has not yet occurred, would have been caused by the defendant's data breach and not the prior data breach. Understanding the totality of difficulties facing plaintiffs in the current environment will assist in determining what a plaintiff should be fairly expected to prove in order to recover for increased risk of identity theft.

A. Deal with the Devil: Implied Contract Claims

Where no express contract exists that imposes liability on a defendant for data breach, plaintiffs have sued for breach of implied contract.[192] The primary difference between an express contract and an implied contract is that in an implied contract, there is no direct evidence of an agreement.[193] An implied contract can be implied in fact, such as through a course of dealing between the parties that supports an implicit agreement to shift liability to one party.[194] An implied contract can also be implied in law, such as through a relationship between the parties or ordinary trade practices that support the imposition of liability by the law in the interest of justice.[195] Once an agreement or obligation is established, the legal effect of an implied contract is the same as that of an express contract.[196]

1. If It Ain't Broke: Lack of Compensable Damages

Courts largely dispense with claims for breach of implied contract because data breach claims do not allege compensable damages as required under applicable state law.[197] Some state law, however, allows for recovery

191. *See generally* Zitter, *supra* note 59.

192. *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).

193. *See* 17A AM. JUR. 2D *Contracts* § 14(e) (2004).

194. *Id.*

195. RESTATEMENT (SECOND) OF CONTRACTS § 4(b) (1981); *see also* 17A AM. JUR. 2D *Contracts* § 14.

196. RESTATEMENT (SECOND) OF CONTRACTS § 4(a).

197. *E.g.*, *Pisciotta*, 499 F.3d at 639-40 (noting that compensable damages are an element of a breach of contract claim under Indiana law, and holding that increased risk of future identity theft is not "a harm that the law is prepared to remedy"); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009) (finding no "showing of appreciable and actual damage" as required for breach of contract under California law).

of mitigation costs that are reasonable and foreseeable.[198] Whether the costs are reasonable and foreseeable depends on an evaluation of the facts of the case and may require a showing of criminal intent or actual identity theft rather than "inadvertently misplaced or lost data."[199]

2. No Deal: Existence of Implied Contract

The existence of an implied contract is fundamental to a claim for its breach. Some courts have found that a contract was "implied in fact" when a customer used a credit or debit card in a commercial transaction—presumably with the agreement of the vendor to take "reasonable measures to protect the information."[200] Other courts, however, have not found an implied contract on the basis of public statements emphasizing a defendant's commitment to safeguarding its customer's private information, even when plaintiffs alleged that they would not have supplied their personal information absent such an implied contractual obligation.[201]

As a practical matter, plaintiffs in those cases failed to allege that they had read or received and understood the defendant's public statements prior to supplying their personal information.[202] Moreover, plaintiffs did not allege that they relied on the defendant's statements as assent to a contractual obligation when they supplied their personal information.[203] It is unlikely, in a typical commercial transaction for sale of goods or services, that protection of payment information is as essential to obtain assent as the receipt of goods or services themselves. However, where such a commercial transaction already exists, a court may view the obligation to protect a customer's information as an implied condition to the already-existing agreement.[204]

198. *E.g.*, Anderson v. Hannaford Bros. Co., 659 F.3d 151, 162, 166-67 (1st Cir. 2011) (noting that courts in Maine allow for recovery of reasonable mitigation costs, and holding that costs to obtain replacement debit and credit cards and costs of identity theft insurance were reasonable under the facts of the case).

199. *Id.* at 164 ("This case involves a large-scale criminal operation . . . and the deliberate taking of credit and debit card information by sophisticated thieves . . . . Here, there was actual misuse, and it was apparently global in reach.")

200. *E.g.*, *id.* at 159; *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011).

201. Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS, 2013 WL 440702, at *20-21 (N.D. Ga. Feb. 5, 2013); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199-1200 (D.N.D. 2004).

202. *Willingham*, 2013 WL 400702, at *20-21; *Dyer*, 334 F. Supp. 2d at 1199-1200.

203. *Willingham*, 2013 WL 400702, at *20-21; *Dyer*, 334 F. Supp. 2d at 1199-1200.

204. *Cf.* Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 795-96 (N.D. Ohio 1965) (recognizing an "implied promise of secrecy" in a doctor-patient contract based on

Courts may imply a contractual duty to protect customer information because of public policy reasons. For example, courts have found an implied condition to protect client information in the doctor-patient relationship,[205] but not in the context of a typical claim for data breach. The deeply confidential nature of the relationship between a patient and her doctor may compel the court to recognize the implied condition; the doctor-patient relationship is fundamentally based on trust and confidentiality because the promise of confidentiality encourages patients to fully disclose even the most embarrassing details of their lives in order to receive effective medical care.[206] By comparison, the relationship between a typical commercial vendor and a customer is not subject to the same public policy considerations. The underlying interest in protecting doctor-patient relationships is to encourage public health and safety, whereas creation of a similar obligation in a typical commercial transaction would merely seek to protect a customer's finances.

3. We Didn't Start the Fire: Proving Causation

Even if a court recognizes a contractual obligation in a Data Breach Claim, the plaintiff must still show a causal relationship between the defendant's breach and the plaintiff's injury.[207] There is no detailed analysis of the causation element of breach of contract in a setting for increased risk of identity theft. Even when actual identity theft occurs, this may not be easy—a plaintiff must plead more than the fact that identity theft occurred after a data breach.[208]

For example, both the Eleventh and Ninth Circuits held that a causal connection between data breach and actual identity theft was sufficiently plead when plaintiffs alleged that they had not previously been the victims of identity theft, that they were very careful in securing their private information, and that the information lost in the defendant's data breach

public policy considerations). Note, however, that the public policy considerations arising from a doctor-patient contract generally do not arise between parties in a Data Breach Claim.

205. *Id.*

206. *Id.* at 801-02; *see also* Susan Dorr Goold & Mack Lipkin, *The Doctor-Patient Relationship: Challenges, Opportunities, and Strategies*, 14 J. GEN. INTERNAL MED. S26, S32 (1999), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1496871/pdf/jgi_267.pdf ("The expectation of privacy is one of the most important aspects of the doctor-patient relationship and influences the disposition to trust.").

207. Resnick v. AvMed, Inc., 693 F.3d 1317, 1325 (11th Cir. 2012).

208. *Id.* at 1326-27 (citing Stollenwerk v. Tri-W. Health Care Alliance, 254 F. App'x 664, 667-68 (9th Cir. 2007)).

was the same type of information used to steal their identities.[209] These requirements may be helpful in pleading causation for the increased risk of identity theft. However, this standard is not helpful to a plaintiff who suffered identity theft prior to the data breach. As an alternative, it would be logical for such a plaintiff to be required to show that the defendant's data breach is more likely to be the cause of the identity theft than whatever circumstances gave rise to a previous identity theft. For example, if the recent identity theft involved the use of the plaintiff's social security number, but the prior identity theft was caused by misuse of the plaintiff's credit card information (and the plaintiff's social security number was not previously compromised), then the recent theft would more likely result from the defendant's data breach.

The standard of proving causation for identity theft is open to substantial criticism. Even if a plaintiff can show that he was not previously the victim of identity theft, that he exercised care in protecting his personal information, and that the data compromised in the breach was the same data used in the identity theft, he has not shown that the identity theft is not as likely to have resulted from some other third party's loss or sale of his information.[210] This criticism applies somewhat in the context of a claim for only increased risk of identity theft. If many third parties could potentially be responsible for the compromise of a plaintiff's data that may lead to identity theft, then credit-monitoring services would be no more necessary after the defendant's data breach than they would have been absent the defendant's data breach.

On the other hand, requiring a plaintiff to prove that no other third party may have been responsible for some increased risk of identity theft is impractical because it requires in-depth investigation of whether any third parties that have access to the same information experienced data breaches. Not all of those third parties may have reported a data breach and not all of those third parties are necessarily aware of data breaches that occurred. For example, a plaintiff's social security number may be in the databases of utility companies, cell phone carriers, banks, and current or prior employers.[211] Moreover, other third parties whom the plaintiff does not even know may have caused increased risk of identity theft by erroneously

209. *Id.* at 1327; *Stollenwerk*, 254 F. App'x at 668.

210. *Resnick*, 693 F.3d at 1330-31 (Pryor, J., dissenting) (arguing that the plaintiff had not sufficiently plead causation to have crossed the line "'from conceivable to plausible,'" and that the complaint was thus subject to dismissal pursuant to Federal Rule of Civil Procedure 12(b)(6) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 680 (2009))).

211. Kiviat, *supra* note 4.

entering another person's data or randomly using the plaintiff's data in an attempt to evade law enforcement action.[212]

At the opposite end of the spectrum of proving causation, a court could find that any proven data breach automatically causes increased risk of identity theft. Just as the risk of being in an automobile crash is increased by virtue of simply being on the roadway, a misplaced hard drive or erroneous email attachment increases the risk of identity theft. Of course, such a loose standard for causation would render the requirement meaningless. A court could require a plaintiff to show that he would not require credit-monitoring services *but for* the defendant's data breach.[213] Alternatively, a court could require a plaintiff to show that the defendant's data breach was a substantial factor in the plaintiff's increased risk of identity theft.[214] In this standard, the plaintiff's general habits in protecting his data would help determine whether the defendant's data breach significantly contributed to the plaintiff's risk of identity theft or if the data breach was just a drop in the bucket.[215]

B. A Tort of Course: Claims of Negligence

The elements of a negligence claim vary by jurisdiction, but the common breakdown involves a tortfeasor's duty to the victim, a breached standard of care, and factual/proximate causation of actual damages.[216] Factual causation and actual damages face the same evidentiary obstacles in negligence claims as in claims for breach of contract.[217] Further difficulties may arise in establishing breach of the standard of care and proximate cause.

1. (Data) Breach of Standard of Care

One requirement of negligence is that the tortfeasor's conduct must deviate from that of a reasonable prudent person.[218] In the case of a data breach, the deviation in question would be from what a reasonable prudent

212. Bob Sullivan, *Odds Someone Else Has Your SSN? One in 7*, NBC NEWS (Dec. 3, 2010), https://web.archive.org/web/20140205224709/http://www.nbcnews.com/technology/odds-someone-else-has-your-ssn-one-7-6C10406347.

213. *See But-For Test*, BLACK'S LAW DICTIONARY 228 (9th ed. 2009).

214. *See Substantial-Cause Test*, BLACK'S LAW DICTIONARY 1566 (9th ed. 2009).

215. *See id.*

216. David G. Owen, *The Five Elements of Negligence*, 35 HOFSTRA L. REV. 1671, 1671-72 (2007).

217. *E.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635, 639-40 (7th Cir. 2007); Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009); *see supra* Part III.A.

218. Owen, *supra* note 216, at 1677.

data holder would do to protect the data in its possession. If the data holder breached an agreement with its client regarding data security, then a breach of contract claim would apply. In the absence of a breached agreement, standards for the data-holder's conduct may be developed from applicable regulations[219] and industry-specific custom.[220]

a) Current Data Security Regulations

A statutorily defined standard of care must describe reasonable security measures with enough specificity to be of any assistance beyond establishing a duty to exercise reasonable care.[221] However, no current regulation mandates standards with any helpful specificity.[222] For example, California's Security Breach Information Act, which serves as a model in other jurisdictions, imposes a duty on data holders.[223] Yet even this statute only requires a business to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[224] The generality of the statutory language does not help a business determine what level of data encryption or security software to use. Instead, whether the business used "reasonable security procedures and practices"—a standard with no more meaning than conduct of a reasonable prudent person—is left to the trier of fact to determine with no guidance.[225]

Both the White House and the Federal Trade Commission (FTC) have recognized the need for security standards. In its February 2012 recommendation for "A Framework for Protecting Privacy," the White House advocated for members of various industries or interest groups to

219. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 264 (2005) ("A statute may impose a duty to exercise care to protect data from intruders, either by the legislation's express terms or by a court's holding that a statute which is silent as to civil liability sets the appropriate standard of care for a tort action.") (citations omitted).

220. *E.g.*, Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1071 (2009) (discussing industry self-regulation vis-à-vis credit card companies establishing security guidelines to which merchants must conform).

221. Johnson, *supra* note 219, at 265-268.

222. Cave, *supra* note 24, at 781-82.

223. Johnson, *supra* note 219, at 264-65.

224. CAL. CIV. CODE § 1798.81.5(b) (West 2006), *amended by* 2014 Cal. Legis. Serv. Ch. 855 (West) (modifying the businesses included under the subsection to include those which own, license, *or maintain* personal information).

225. Johnson, *supra* note 219, at 265.

collaborate and develop governing codes of conduct.[226] The codes would not result in binding regulation, but would provide a standard to which the FTC may refer in enforcement actions.[227] By keeping development and maintenance of the codes in the control of the "stakeholders," the White House intended to encourage stakeholder commitment, allow agile adjustment in a "rapidly evolving marketplace," and help stakeholders build consumer trust.[228]

The FTC released a report in March 2012 ("the Final Report") that encouraged the development of baseline privacy legislation.[229] The legislation would be intended to provide security standards for those data holders that did not already have minimum standards and enforce the standards against companies that intentionally ignored them.[230] The proposed legislation would "provide adequate deterrence through the availability of civil penalties and other remedies."[231] However, the recommendations made no specific reference to providing a private right of action or remedy that would directly benefit the data subjects.[232] Still, as a set of "minimum standards," such legislation may be helpful to a trier of fact in determining whether conduct breaches a standard of care.

b) Other Sources of Standards

In the meantime, fact finders must rely on evidence such as industry norms from other data holders of similar size and purpose or internal records regarding security procedures. However, many industries do not establish norms that are consistently implemented, and courts may not even recognize basic security safeguards.

For example, the Federal District Court for the District of Minnesota found no breach of duty when the laptop of a student loan company

226. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 23-24 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

227. *Id.* at 24.

228. *Id.*

229. Chiu, *supra* note 24, at 299 (citing FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf).

230. FED. TRADE COMM'N, *supra* note 229, at 12-13.

231. *Id.* at 13.

232. *See id.*

employee was stolen during the burglary of his home.[233] The laptop contained unencrypted data on the company's customers, including names, addresses, social security numbers and loan balances.[234] The company notified all of its customers of the breach because the employee did not keep track of exactly what data was permanently saved on the laptop's hard drive.[235]

The plaintiff alleged that the company breached its duty of reasonable care "by (1) providing [the employee] with [personal information] that he did not need for the task at hand, (2) permitting [the employee] to continue keeping [personal information] in an unattended, insecure personal residence, and (3) allowing [the employee] to keep [personal information] on his laptop unencrypted."[236] The plaintiff additionally asserted that this conduct violated the Gramm-Leach-Bliley Act, which requires companies to develop and implement their own data security procedures.[237]

The district court concluded that the company did not breach a duty of reasonable care because the company had security procedures and authorized the employee to access the data pursuant to his duties.[238] Because the Gramm-Leach-Bliley Act does not specifically require that personal information be encrypted, the district court declined to find a breach based on violation of the statute.[239]

The plaintiff additionally alleged negligent behavior with respect to the company's own policy of "restrict[ing] access to nonpublic personal information to authorized persons who need to know such information."[240] Once again, the district court agreed that because the company complied with its own procedures in training the employee to handle the data, and because those procedures were presumably not violated, no breach occurred.[241]

The district court's findings are disturbing because they appear to rely solely on the defendant's own internally developed policies to determine a

233. Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3-5 (D. Minn. Feb. 7, 2006).

234. *Id.* at *1-2.

235. *Id.*

236. *Id.* at *4 (citations omitted) (internal quotation marks omitted) ("personal information" alteration in original).

237. *Id.* at *3-4 (citing the Gramm-Leach-Bliley Act (GLB Act), 15 U.S.C. § 6801 (2012)).

238. *Id.* at *4-5.

239. *Id.*

240. *Id.* at *4.

241. *Id.*

standard of reasonable conduct. However, a search for a more objective industry standard or "best practice" could have led a fact finder to disagree. For example, one security company has circulated "Laptop Security Best Practices" that recommends encryption of all customer records,[242] cable locks for laptops in the home,[243] and disk-wipe technology in case of loss or theft.[244]

Litigators should arm themselves with similar bases for best practices. Otherwise, when companies who experience data breaches have not violated a statute or their own internal security policies, courts have little guidance as to what constitutes failure to exercise reasonable care.

2. Proximate Cause

Where a data breach occurs as a result of a third party's criminal act, plaintiffs in data breach cases have further difficulties proving that the defendant's negligence proximately caused the breach. As the district court for the District of Minnesota recited, "As a general rule, the criminal act of a third party is an intervening efficient cause sufficient to break the chain of causation, provided that the criminal act was not foreseeable and there was no special relationship between the parties."[245] As data breaches become more commonplace, the intervening act may be more foreseeable, but burglary of a home in a "relatively safe" neighborhood resulting in laptop theft is not foreseeable.[246] Thus, criminal acts may break the chain of causation if they were not foreseeable. If a burglary of a home in a "relatively safe" neighborhood was not foreseeable, perhaps hacking into a relatively secure server is similarly unforeseeable.

IV. There Must Be Some Kind of Way Out of Here

As the number of people affected by data breaches continues to rise,[247] public awareness of data breaches and backlash against those with whom

242. PC GUARDIAN, LAPTOP SECURITY BEST PRACTICES 3 (2007), *available at* http://www.securitysolutions.ca/resources/PCGuardian/Laptop_Security_Best_Practice_White_Paper.pdf.

243. *Id.* at 6.

244. *Id.* at 7.

245. *Guin*, 2006 WL 288483, at *6 (citation omitted) (internal quotation marks omitted).

246. *Id.*

247. Herb Weisbaum, *Data Breaches Cost Consumers Billions of Dollars*, TODAY MONEY (June 5, 2013), http://www.today.com/money/data-breaches-cost-consumers-billions-dollars-6C10209538.

consumers trust their information has also risen.[248] Identity theft rates are rising[249] and victims of data breaches face much larger chances of becoming fraud victims than others.[250] As the parties who are best positioned to safeguard against data breaches, businesses should bear the weight of the liability.

A. Indecent Proposals: Current Suggestions for Solutions

In the current environment, plaintiffs have little to no chance of recovering for a data breach claim. Not only is there difficulty in establishing the prima facie elements of a common law tort,[251] but courts may not even recognize standing to sue for increased fraud risk.[252]

Some scholars propose that the threshold standing issue should be addressed by rejecting the Third Circuit's position.[253] Others propose comprehensive privacy legislation that includes a private right of action and an explicit grant of authority to the FTC to establish and enforce business privacy practices.[254] Congress should establish a statutory right of action that adopts the Third Circuit's test for standing. While the statute may authorize the FTC to promulgate guidelines for businesses to follow, the right of action should clearly demarcate the types of conduct that create liability, regardless of meeting FTC guidelines.

Currently, the FTC enforces privacy standards by prosecuting enforcement lawsuits pursuant to section 5 of the FTC Act.[255] This provision authorizes the FTC to prevent various entities from engaging in "unfair or deceptive acts or practices in or affecting commerce."[256] Under the "deceptive acts" prong of section 5, the FTC prosecutes breaches of

---

248. *E.g.*, Martha C. White, *Cost of Data Breach Could Give Target Sticker Shock*, NBC NEWS (Jan. 10, 2014), *available at* https://web.archive.org/web/20140111024900/http://www.nbcnews.com/business/cost-data-breach-could-give-target-sticker-shock-2D11899205 (discussing the public backlash on social media websites).

249. *See* Richard Rubin, *Criminal Identity Theft Investigations Rise 66% at IRS*, BLOOMBERG (Jan. 7, 2014), http://www.bloomberg.com/news/2014-01-07/criminal-identity-theft-investigations-rise-66-at-irs.html.

250. Weisbaum, *supra* note 247 ("Someone who's had their data breached is 14 times more likely to become a fraud victim . . . .")

251. *See supra* Part III.

252. *See supra* Part II.

253. *E.g.*, Galbraith, *supra* note 14, at 1398-99 ("[A]lthough data breach victims may fail to recover damages at trial . . . [they] deserve their day in court.")

254. Cave, *supra* note 24, at 789-90.

255. *See* Chiu, *supra* note 24, at 287-88; *see also* FED. TRADE COMM'N, *supra* note 229, at vi, 24.

256. 15 U.S.C. § 45(a) (2012).

privacy statements.[257] The FTC has also used the "'unfair practices'" prong against companies "that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information."[258] Authority to enforce privacy rights under the "unfair practices" prong has, however, come under recent attack in federal court.[259]

If Congress grants express authority to the FTC to establish and enforce data security guidelines, businesses will receive more guidance as to how to protect consumer data.[260] The threat of enforcement with civil fines will deter businesses from deliberately putting consumer data at risk of exposure.[261] However, provision of data security guidelines alone does not provide a mechanism for recovery by injured parties. Furthermore, compliance with administrative guidelines may preempt recovery in cases where a data holder's conduct warrants liability. Rather than evaluate possible negligence based on the facts before a court, the court may presume that compliance with FTC guidelines equates to conformity with a standard of care—even if the guidelines merely establish a "floor" of data security measures.[262]

B. Jumping Hurdles: Requirements for an Effective Private Right of Action

Data breach victims need a private right of action that removes unreasonable and unpredictable barriers to recovery. Furthermore, data holders need guidance on how best to protect their customers' data and reduce risk of liability for data breaches.

1. Standing Strong

A statutory right of action represents Congress's acknowledgement of a legally redressable injury.[263] In this case, the newly cognizable injury is increased risk of identity theft. However, the injury recognized in the

257. THE WHITE HOUSE, *supra* note 226, at 27, 27 n.32.

258. David J. Bender, Essay, *Tipping the Scales: Judicial Encouragement of a Legislative Answer to FTC Authority over Corporate Data-Security Practices*, 81 GEO. WASH. L. REV. 1665, 1666, 1668 (2013) (quoting *Making Sure Companies Keep Their Privacy Promises to Consumers*, FED. TRADE COMMISSION, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited Dec. 14, 2014)).

259. *Id.* at 1676-83 (advocating judicial recognition of FTC authority in light of pending litigation).

260. FED. TRADE COMM'N, *supra* note 229, at 12.

261. *Id.*

262. *Cf.* Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4-5 (D. Minn. Feb. 7, 2006).

263. *See supra* Part II.A.

statute must be particularized in order to remain within the boundaries of Article III.[264] Thus, the private right of action should be provided for plaintiffs whose information was subject to a data breach. If no data breach has occurred, a plaintiff cannot bring an enforcement action against his or her data holder to prevent a data breach, even if the statute authorizes it. Such a plaintiff would not have a sufficiently particularized injury to satisfy constitutional standing requirements.

The idea of taking action to prevent a data breach seems favorable compared to making a plaintiff wait until his or data is irreversibly compromised. But allowing a consumer to prosecute an enforcement action would not only fail to provide standing, it would effectively allow consumers to unnecessarily interfere with the management of many data holders' security procedures. Furthermore, in order to ensure that suits brought under the proposed statute are limited to plaintiffs who actually suffer increased risk of identity theft, the statute should incorporate the standing requirements of the Third Circuit. To wit, a plaintiff should be able to show that the perpetrator of a data breach "(1) read, copied, and understood [the plaintiffs'] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [plaintiffs'] names."[265]

The Third Circuit's test, in effect, allows only actual victims to sue for a data breach—not just anyone who suspects his or her data was compromised in the hands of a company. The test also ensures that plaintiffs suffer actual increased risk of identity theft by requiring that the compromised information could even be used for identity theft. Rather than turn plaintiffs away at the courthouse steps, the Third Circuit test imposes basic requirements of plausibility to the alleged injury.

Because standing requirements should not be unduly burdensome in facilitating access to courts, application of the Third Circuit's test need not be painstaking. For example, a showing of intent to misuse compromised information may be satisfied by showing that the plaintiff's information was the only data (or in one of a few categories of data) that was compromised. To show that the plaintiff's data was "understood," a plaintiff may be required to show that the data was in an understandable format, such as with little or no encryption.

---

264. *See supra* Part II.A.

265. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

By adopting the Third Circuit's standing requirements, a statutory right of action would allow plaintiffs access to the courts in a manner consistent with emerging case law. The requirements impose a low burden of plausibility to ensure actual injury in fact. Simultaneously, legislative recognition of increased risk of identity theft as a legally cognizable injury promotes consistent recognition of standing, especially in lower courts that may not yet recognize standing for data breach claims.

2. The Common Law Obstacle Course

a) Damages

Currently, data breach claims that survive challenges to standing fail for lack of compensable damages.[266] The easiest way to remedy this issue is to provide for recovery of costs listed in the statute. Plaintiffs should recover for actual reasonable costs incurred for credit-monitoring services.

Courts should evaluate the ability of credit-monitoring services to adequately remedy increased risk of identity theft in light of a variety of factors. For example, the type of data compromised may affect the level of risk to which the plaintiff is exposed and warrant more comprehensive credit monitoring. The type of data compromised may also affect the length of time for which credit monitoring is reasonable. A compromised social security number will require longer and more intense monitoring than a home address or license plate number. Also, the amount that the plaintiff stands to lose or for which the plaintiff may be liable may warrant more comprehensive credit monitoring. Thus, characteristics like assets and available credit may factor into a claim's value. If the data holder has already offered to pay for credit-monitoring services, the plaintiff's decision to either forego that service or obtain additional services may also factor into whether the cost is reasonable.[267]

Additionally, plaintiffs should recover for reasonable time spent safeguarding against identity theft as a result of a data breach. Time spent safeguarding against identity theft may include reasonable time spent contacting banks to change account numbers, contacting credit bureaus to initiate fraud alerts, and taking other remedial measures specifically in response to notification of the data breach.

---

266. *See supra* Part III.A.1.

267. As an aside, it may be advisable for data holders who have experienced data breaches to offer credit-monitoring services with a disclaimer of liability for increased risk of identity theft.

b) Standard of Care

Comprehensive regulatory guidelines could give businesses guidance on best practices for data security.[268] Development of guidelines must account for changes in technology across a broad spectrum of types and sizes of data holders.[269] The FTC may be on track to obtain authority to establish and enforce guidelines,[270] and time will tell if the FTC is successful in promulgating agile and effective guidelines.

Regardless of the efficacy of FTC regulations, the statutory right of action should clarify that liability does not rest solely on noncompliance with the guidelines. The guidelines should factor prominently in any analysis of liability, but courts must retain discretion to judge data holder liability regardless of regulatory compliance or violation. Judicial discretion allows for consideration of facts unique to any situation, which may not have factored into the guidelines. Discretion also reduces the probability of reliance on bad guidelines.

Allowing for liability regardless of compliance with regulatory guidelines creates some uncertainty for businesses as to whether their conduct is sufficient to avoid liability. But judicial discretion also allows data holders to avoid liability despite noncompliance where abnormal situations may warrant it. Furthermore, absence of discretion robs the judicial process of meaning; courts should have authority to dispense justice according to reason and policy as well as guidance from regulatory agencies.

V. Conclusion: All Along the Watchtower

Rapid changes in technology and in the extent to which individuals place their sensitive information at the mercy of third parties have outpaced the ability of the government to keep up. As a result, victims of data breaches have been left in the cold with no recourse. But with the help of Congress and the FTC in outlining privacy rights, those victims can regain control

268. Cave, *supra* note 24, at 787-89.

269. THE WHITE HOUSE, *supra* note 226, at 6-7.

270. *See* Press Release, Fed. Trade Comm'n, Testifying Before the Senate Judiciary Committee, FTC Reiterates Its Support for Data Security Legislation (Feb. 4, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/testifying-senate-judiciary-committee-ftc-reiterates-its-support ("The Commission supports legislation, for example, that would give the FTC the ability to seek civil penalties to help ensure FTC enforcement actions have an appropriate deterrent effect.")

and prosecute those rights in a judicial system that has addressed thorny issues with practicality and judiciousness for centuries.

Elizabeth T. Isaacs