American University Law Review

Volume 62 | Issue 5 Article 7

2013

Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information

Miles L. Galbraith
American University Washington College of Law

Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information

Keywords
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, Ceridian Corp. -- Trials, litigation, etc., Hacking (Computer security), Identity theft -- Prevention, Locus standi -- United States, Data security failures -- Lawsuits & claims, Personal information management -- Law & legislation, Torts -- United States -- Cases, Damages (Law) -- United States

COMMENT

IDENTITY CRISIS: SEEKING A UNIFIED APPROACH TO PLAINTIFF STANDING FOR DATA SECURITY BREACHES OF SENSITIVE PERSONAL INFORMATION

MILES L. GALBRAITH*

Today, information is largely stored and transmitted electronically, raising novel concerns about data privacy and security. This data frequently includes sensitive personally identifiable information that is vulnerable to theft and exposure through illegal hacking.

A breach of this data leaves victims at a heightened risk of future identity theft. Victims seeking to recover damages related to emotional distress or money spent protecting their identities and finances are often denied Article III standing to pursue a claim against the entity charged with protecting that data. While the U.S. Court of Appeals for the Seventh Circuit in Pisciotta v. Old National Bancorp *and the U.S. Court of Appeals for the Ninth Circuit in* Krottner v. Starbucks Corp. *recognized standing even when harm was limited to the increased risk of identity theft, the U.S. Court of Appeals for the Third Circuit in* Reilly v. Ceridian Corp. *split with its sister courts and denied standing for data breach victims, citing a lack of injury-in-fact.*

The Reilly *court's application of the standing doctrine creates an unreasonable barrier for injured plaintiffs to reach the merits of their*

* Junior Staff Member, *American University Law Review*, Volume 62; J.D. Candidate, May 2014, *American University Washington College of Law*, B.A., English, 2007,*University of California Santa Barbara*. Thanks to Professor Steven Wermiel for his guidance and to my fellow *AULR* staff for their skillful editing, particularly Peter Frechette, Kat Scott, Allison Vissichelli, John Forbush, Brian Shearer, Amanda Smith, Adelia Hunt, Michael Castle Miller, Anna Lashley, Chad Guo, and Elyse MacNamara. Finally, I am deeply grateful to my parents Mark and Debra Galbraith, my brother Evan, and my wife Laura Updegrove, for their love and support.

cases. The circuit split should be resolved in favor of conferring standing for those who suffer a threat of future harm. Data breach plaintiffs' standing should be recognized, just as the plaintiffs' standing in "latent harm" tort law cases is recognized, because the increased risk of future harm in defective medical device, toxic substance exposure, and environmental injury cases is logically analogous and applicable to the increased risk of harm in data breach cases. In addition, the Supreme Court's original purpose of the standing doctrine supports acknowledging that the risk created by a data breach and the resulting expenses to protect against identity theft constitute a real, present, particularized injury worthy of justiciability.

TABLE OF CONTENTS

Introduction 1366
I. Background 1372
A. History and Prevalence of Data Security Breaches 1372
B. Article III Standing Requirements and Injury-in-Fact 1375
C. Lower Court Decisions and the Initial Trend Toward Denying Standing in Data Breach Cases 1378
D. The New Circuit Split 1380
II. Data Breach Plaintiffs Should Not Be Turned Away at the Courthouse Steps 1384
A. The Supreme Court's Standing Doctrine Permits Justiciability of Data Breach Victims' Claims 1384
B. Application of Analogous "Latent Harm" Tort Law Principles to Standing in Data Breach Cases Compels a Finding of Article III Standing 1386
1. Toxic exposure 1386
2. Defective medical devices 1389
3. Environmental harm 1391
C. The Economic Loss Rule Should Not Bar Recovery of Damages in Data Security Claims and Is Irrelevant to the Standing Analysis 1394
Conclusion 1396

INTRODUCTION

"We have built our future upon a capability that we have not learned how to protect."[1] These words, spoken by former CIA Director George Tenet, acknowledge the critical vulnerabilities of information-age technology on which we rely in modern society. Information in the modern

1. *See* Robert O'Harrow, Jr., *Understanding Cyberspace is Key To Defending Against Digital Attacks*, WASH. POST (June 2, 2012), http://www.washingtonpost.com/investingations/understanding-cyberspace-is-key-to-defending-against-digital-attacks/2012/06/02/gJQAsIr19U_story.html (quoting former CIA Director George Tenet).

world is increasingly stored and transmitted electronically, rapidly replacing the methods of the past.[2] While electronically storing data comes with extraordinary environmental and economic advantages,[3] its use raises novel concerns about the privacy and security of digital data.[4]

Much of the electronic information stored in databases by corporations and organizations includes sensitive personal information, such as social security numbers, phone numbers, birthdates, addresses, financial records, and medical records.[5] Electronic data is uniquely vulnerable to theft and exposure on a catastrophic scale.[6] Private electronic data can be exposed through illegal hacking,[7] employee theft,[8] the loss of laptops and hard drives,[9] and even through inadvertent exposure on the Internet.[10] It is clear

---

2. *See id.* (observing that data stored in online networks "is a vital reality that includes billions of people, computers and machines," and that "[a]lmost anything that relies on code and has a link to a network could be a part of cyberspace"); *see also* Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 184 (2011) (observing that "[a]s the volume of [digitally stored] data has increased, so have the instances of hacking and computer theft that result in personal information being exposed").

3. *See* PAUL BARBER & BOB WEST, UNISYS, THE "PAPERLESS" BANK—A REALITY, ADVISORY REPORT: BUILDING AN EFFICIENT WORKFORCE AND A POWERFUL CUSTOMER EXPERIENCE (2008), *available at* http://www.unisys.com/unisys/common/download.jsp?d_id=9000046&backurl=/unisys/ri/pub/bl/detail.jsp&id=9000046 (extolling the increased efficiency and profitability resulting from the digitization and automation of banking documents); Ned Madden, *Sustainability Software, Part 2: Cutting the Paper Chase*, TECH NEWS WORLD (Dec. 8, 2009, 4:00 AM), http://www.technewsworld.comstory/68834.html (explaining how using paperless business processes reduces environmental harm and is economically efficient).

4. *See* Abraham Shaw, *Data Breach: From Notification To Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 517–18 (2010) (observing that "[b]ecause private information is increasingly available over the internet, there is a rising demand for data breach laws that protect private information").

5. Carolyn A. Deverich et al., *Into the Breach*, L.A. LAW., Feb. 2012, at 27 (outlining the wide variety of personally identifiable data that is stored and transmitted online and vulnerable to exposure).

6. *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., MDL No.11md2258, 2012 WL 4849054, at *1 (S.D. Cal. Oct. 11, 2011); *see also* Liana B. Baker & Jim Finkle, *Sony PlayStation Suffers Massive Data Breach*, REUTERS (Apr. 26, 2011), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426 (reporting the potential compromise of the confidential account and financial information of millions of Sony PlayStation, Qriocity, and Sony Online Entertainment Network users, including unencrypted credit card numbers).

7. *See, e.g.*, *In re* TD Ameritrade Accountholder Litig., 266 F.R.D. 418, 419 (N.D. Cal. 2009) (denying final approval of the proposed settlement after TD Ameritrade suffered a security breach that exposed private information of account holders); David Kravets, *Ameritrade Hack Settlement: $2 per Victim, $1.8 Million for Lawyers*, WIRED (July 11, 2008, 11:55 AM), http://www.wired.com/threatlevel/2008/07/ameritrade-hack/ (explaining how the data theft "gave hackers access to customer names, phone numbers, e-mail accounts and home addresses").

8. *See* Brian Krebs, *Data Theft Common by Departing Employees*, WASH. POST (Feb. 26, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html (highlighting the frequency at which former employees stole items such as business information, customer contact lists, employee records, and financial information).

9. *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (detailing

that few entities that use online or electronic databases are impervious to data loss, given that between eighty to ninety percent of Fortune 500 companies and government agencies have experienced data breaches of some type.[11] Electronic data breaches have become a leading cybersecurity challenge for the private and public sectors alike.[12]

With the increased use of digital data storage, the frequency and severity of breaches of data security are on the rise,[13] and correspondingly, litigation relating to the exposure of personal data has increased.[14] Some estimates put the number of records breached since 2005 at over 600 million.[15] A breach of personally identifying digital information leaves victims at a heightened risk of future identity theft and misuse of their private

---

how a laptop containing employee personal data was stolen from a Starbucks store); Jaikumar Vijayan, *BP Employee Loses Laptop Containing Data on 13,000 Oil Spill Claimants*, COMPUTERWORLD (Mar. 29, 2011, 8:22 PM), http://www.computerworld.com /s/article/9215316/BP_employee_loses_laptop_containing_data_on_13_000_oil_spill_ claimants (reporting on an incident where "[t]he personal information of 13,000 individuals who had filed compensation claims with BP after [the Deepwater Horizon] oil spill may have been compromised after a laptop containing the data was lost by a BP employee"). The lost computer contained claimants' names, social security numbers, addresses, phone numbers, and birth dates, all stored in unencrypted files. Vijayan, *supra*.

10. *See, e.g.*, Dori Saltzman, *Update: Cruise Line Data Breach Exposes 1,200-Plus Passengers*, CRUISECRITIC (June 26, 2012, 7:30 AM), http://www.cruisecritic.com/news/ news.cfm?ID=4878 (reporting on the accidental exposure of cruise line passengers' personal information, such as names, e-mail addresses, and passport numbers, when a spreadsheet containing the information was unintentionally attached to an e-mail sent to a portion of the registered members on the online booking service).

11. *Security Breach Notification Requirements: Guidelines and Securities Law Considerations*, JONES DAY LLP (Mar. 2006), http://www.jonesday.com/Security-Breach-Notification-Requirements-Guidelines-and-Securities-Law-Considerations-03-21-2006.

12. *See, e.g.*, IDENTITY THEFT RES. CTR., 2011 DATA BREACH STATS 1–12 (Feb. 7, 2011), *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_ Stats_Report_2011_20120207.pdf (compiling electronic data breach incidents across business and financial entities as well as a broad array of government and military institutions).

13. *See* Rancourt, *supra* note 2, at 185 (observing how the increasingly frequent data breaches have received prominent media coverage, revealing the growing threat to consumers' private information); *see also* Deverich, *supra* note 5, at 27 (noting that "the frequency of data security breaches has skyrocketed" over the last several years).

14. Timothy H. Madden, *Data Breach Class Action Litigation—A Tough Road for Plaintiffs*, BOS. B.J., Fall 2011, at 27 ("[Data breaches have] increasingly resulted in litigation, often brought as a class action on behalf of all of the hundreds, thousands or even tens of thousands of individuals whose personally identifiable information has been compromised.").

15. *See Chronology of Data Breaches: Security Breaches 2005—Present*, PRIVACY RIGHTS. CLEARINGHOUSE (May 12, 2013), https://www.privacyrights.org/data-breach (identifying 607,472,154 records breached as a result of 3,679 data breaches that have occurred since 2005). This explosion of data security breaches, and the subsequent increased risk of future identity theft for exposed consumers, has fueled a growth in the industry of companies that provide credit-monitoring and identity theft prevention services. *See Identity Theft Protection Services Review*, TOPTENREVIEWS, http://identity-theft -protection-services-review.toptenreviews.com (last visited June 15, 2013) (surveying a wide array of identity theft prevention services such as LifeLock, Identity Force, ProtectMyID, and IdentityGuard).

information.[16]

Victims whose private information has been exposed or compromised often bring legal claims despite a lack of actual fraudulent use of their information.[17] Instead, these plaintiffs claim a present injury suffered as a consequence of an increased risk of harm that may occur in the future.[18] These claims are based on the heightened risk of future identity theft, and the plaintiffs seek to recover damages related to their emotional distress and aggravation, time and money spent protecting their financial accounts, and expenses incurred monitoring their credit to ensure against identity theft.[19]

Frequently, the victims of data security breaches are denied standing to pursue a claim.[20] Under Article III, section 2 of the U.S. Constitution, a plaintiff must establish that he or she has suffered an injury that is concrete, and not hypothetical, in order to achieve standing to sue.[21] Lower courts inconsistently interpret Article III standing requirements in data breach circumstances,[22] and plaintiffs frequently fail to establish standing.[23]

---

16. *See* Deverich, *supra* note 5, at 27–28 (warning that the breach of a person's sensitive data results in an "immediate and immeasurable injury" that creates a violation of personal privacy, a greater risk of identity theft, and a threat to that person's reputation and financial security).

17. *See* Jay M. Zitter, Annotation, *Liability for Risk of Future Identity Theft*, 50 A.L.R. 6TH 33, 33 (2009) (discussing different claims plaintiffs bring against companies after their private information has been exposed).

18. *See, e.g.*, Anderson v. Hannaford Bros., 659 F.3d 151, 155 (1st Cir. 2011) (seeking damages for emotional distress, time, and energy spent reversing unauthorized charges and the cost of identity theft insurance, among other things); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (acknowledging that the plaintiffs' complaint had not alleged "*completed direct* financial loss" resulting from the security breach); Zitter, *supra* note 17, at 33 (identifying the potential threat of future identity theft and discussing case law that has addressed it as a potential injury).

19. *See, e.g.*, *Pisciotta*, 499 F.3d at 632 (detailing the alleged losses resulting from a failure to protect personal confidential information).

20. *See* Rancourt, *supra* note 2, at 187 (noting that class action lawsuits are the typical method of seeking redress, but have had little success and frequently are dismissed for failure to establish Article III standing).

21. U.S. CONST. art. III, § 2; *see also* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (explaining how over time the Supreme Court has established injury-in-fact as part of an "irreducible" constitutional minimum of standing).

22. *See* Deverich, *supra* note 5, at 28 ("The courts that have addressed the standing issue are split."); Zitter, *supra* note 17, at 33 (observing that some courts recognize standing based on risk of future identity theft, and other courts deny standing on similar facts). *Compare* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009) (recognizing standing for "increased risk of identity theft"), *aff'd*, 380 F. App'x 689 (9th Cir. 2010), *with* Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *1 (D.N.J. 2006) (declining to recognize standing to bring a claim for risk of future identity theft).

23. *See* Madden, *supra* note 14, at 29 (commenting that courts nationwide are reticent to hear cases where the plaintiff class has not shown "actual, demonstrable" economic injury). Courts often hold that mere exposure of personal sensitive data does not constitute injury-in-fact as required to confer standing; instead, plaintiffs must show that the exposed personal data was exploited and that the victim suffered actual financial loss through theft of a compromised bank account or other harm. *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ 6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) (concluding

The question of standing in data breach cases only recently reached the federal courts of appeals, with the persistently unsettled nature of this area of law resulting in a circuit split.[24] While the U.S. Court of Appeals for the Seventh and Ninth Circuits recognize standing based on the future risk of harm, the U.S. Court of Appeals for the Third Circuit has explicitly refused to confer standing to plaintiffs without more. The Seventh Circuit in *Pisciotta v. Old National Bancorp*[25] broke the lower courts' trend of denying standing by recognizing standing for victims of data breaches, even when the harm was limited only to the increased risk of identity theft.[26] In 2010, the Ninth Circuit in *Krottner v. Starbucks Corp.*[27] extended the holding in *Pisciotta*, also conferring standing for data breach victims.[28] However, most recently in the December 2011 decision in *Reilly v. Ceridian Corp.*,[29] the Third Circuit addressed the standing requirement for plaintiffs in data breach cases, denying standing and creating a conflict with its sister courts in the Seventh and Ninth Circuits.[30] The *Reilly* court held that when plaintiffs fail to allege actual misuse of the compromised data, they have neither a "concrete and particularized"[31] injury, nor a threat of harm that is "certainly impending,"[32] as required by the Supreme Court in *Lujan v. Defenders of Wildlife*.[33] Therefore, the Third Circuit ruled that

---

that the plaintiffs lacked standing to bring a claim from accidental loss of back-up computer tapes containing personal information with no allegations of loss or actual damages); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (failing to confer standing for plaintiffs in a hacking incident where there were no allegations of actual harm); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007) (dismissing a claim for lack of standing arising from a stolen laptop where no actual harm was alleged).

24. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (denying standing and establishing a conflict with the holdings in the Seventh and Ninth Circuits), *cert. denied*, 132 S. Ct. 2395 (2012); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (following the Seventh Circuit and recognizing standing); *Pisciotta*, 499 F.3d at 634 (recognizing standing in a case of first impression); *see also* Glenn Lammi, *Federal Circuit Court Goes Its Own Way on Standing in Data Security Class Action*, LEGAL PULSE (Jan. 6, 2012), http://wlflegalpulse.com/2012/01/06/federal-circuit-court-goes-its-own-way-on-standing-in-data-security-class-action (highlighting the decision in *Reilly* from the Third Circuit).

25. 499 F.3d 629, 632 (7th Cir. 2007).

26. *See id.* at 634 (concurring with the view that "the injury-in-fact requirement can be satisfied by a threat of future harm").

27. 628 F.3d 1139 (9th Cir. 2010).

28. *Id.* at 1142. The claim in *Krottner* rested upon an allegation of increased risk of future identity theft stemming from a laptop stolen from a Starbucks coffee shop containing the unencrypted names, social security numbers, and addresses of 97,000 employees. *Id.* at 1140–41. As a matter of first impression for the court, it upheld the notion that when a data breach plaintiff is at an increased risk of harm by identity theft in the future, the plaintiff has suffered injury-in-fact sufficient to confer standing. *Id.* at 1143.

29. 664 F.3d 38, 42 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

30. *See id.* at 44 (rejecting the notion that the courts in *Pisciotta* and *Krottner* discussed a standing requirement applicable to "generalized data theft situations").

31. *Id.* at 41 (quoting Danvers Motor Co. v. Ford Motor Co., 432 F.3d 286, 290–91 (3d. Cir. 2005)).

32. *Id.* at 42 (internal quotation marks omitted).

33. *See id.* at 41–42 (establishing minimum justiciability requirements (citing Lujan v.

the plaintiffs in *Reilly* did not have standing to sue.[34]

This Comment argues that *Reilly* was wrongly decided, misapplied the law, and reached deeply flawed conclusions. Although *Pisciotta* merely hints at a justification for why data breach plaintiffs have standing, and the support in *Krottner* is not adequately developed, the holding in these cases is nonetheless sound.[35] The *Reilly* court raised the low jurisdictional threshold of standing to unjustifiable heights, creating an unreasonable barrier for injured plaintiffs to reach the merits of their cases.

This Comment argues that plaintiffs should be conferred standing because logically-analogous, settled tort law principles apply to the question of standing in data breach cases. When properly interpreted, the Supreme Court's standing doctrine sets a low threshold that does not preclude conferring standing to plaintiffs who face emotional distress or credit-monitoring costs as a consequence of an increased risk of identity theft. The credit-monitoring injunctive relief approved by multiple courts in settlement proceedings between data breach claimants and data storage entities suggests that the threat of identity theft is a remediable injury with concrete available relief.[36] Contrary to the court's analysis in *Reilly*, a robust and sound analogy exists in tort cases that confer standing to plaintiffs on the basis of an increased risk of future harm in defective medical device, toxic substance exposure, and environmental injury cases. Under this reasoning, and applying an analysis that interprets the Supreme Court's original purpose of the standing doctrine, courts should acknowledge a cognizable injury arising from the increased risk of identity theft that is more than simply "conjectural or hypothetical."[37] Cases involving a data breach of sensitive personal information present a clear "case or controversy" to be heard at trial; to deny standing to plaintiffs who suffered due to inadequate data protection is to woefully misapply the standing doctrine.

Defenders of Wildlife, 504 U.S. 555, 560–61 (1992))). The *Reilly* court ruled that even expenditures made by victims to monitor credit information did not confer standing, and that these costs, which were meant to ease the fear of future third-party misuse of victims' information, did not justify standing because any injury was based on a "speculative chain of future events [dependent] on hypothetical future criminal acts." *Id.* at 46.

34. *Id.* at 42.

35. Although the *Reilly* court criticized the reasoning in *Pisciotta* and *Krottner* as "skimpy," those courts merely acknowledged plaintiff standing without the need for extended deliberation. *Id.* at 44.

36. *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 130 (2011) (citing United States v. Janosko, 642 F.3d 40, 42 (1st Cir. 2011)). In *Janosko*, retired Justice David Souter, sitting by designation, opined that it was reasonable for a county whose computer system had been hacked, exposing its employees' private information, to reimburse expenses spent on a credit-monitoring service. *Janosko*, 642 F.3d at 42.

37. Danvers Motor Co. v. Ford Motor Co., 432 F.3d 286, 290–91 (3d Cir. 2005) (citing *Lujan*, 504 U.S. 555).

Part I of this Comment provides a brief overview of the history and development of jurisprudence relating to data security breaches and outlines a number of the most severe breaches that are a part of the dramatic upward trend in recent incidents. This Part also examines the Supreme Court's evolving interpretation of standing requirements, reviews relevant lower court decisions, and explains the results of data breach litigation at the federal appellate level. Part II develops the analytical framework suggested in *Pisciotta* and *Krottner* and analyzes the Supreme Court's line of cases on plaintiff standing, showing that standing should properly be interpreted as a low bar for access to the courts. Part II proceeds by drawing parallels in data breach cases with three analogous areas of tort law—toxic exposures, defective medical devices, and environmental harm—which permit an increased threat of future harm to satisfy the Article III standing requirement for injury-in-fact.

In conclusion, this Comment recommends that the circuit split created by *Reilly* should be resolved by acknowledging the standing doctrine as a low barrier to access to the courts, and the analysis used by the Seventh and Ninth Circuits should be applied to recognize injury-in-fact for plaintiff standing in data breach cases.

I. BACKGROUND

A. History and Prevalence of Data Security Breaches

By virtue of the modern trend in electronic commerce and record keeping, data breaches occur with increasing regularity and practically anyone is vulnerable to exposure.[38] A study conducted by Verizon in conjunction with the U.S. Secret Service in 2011 concluded that incidents of reported data breaches continue to reach new highs: reported incidents from 2010 totaled almost 800, a sharp increase from the 900 breaches reported in the previous six years combined.[39] According to the study, because companies increasingly rely on technology in their everyday business, virtually every major industry is now afflicted with data security breaches.[40] Among the worst affected are the financial services, hospitality, and retail industries, with recent expansion to government institutions and the healthcare industry.[41] The Federal Bureau of

38. Shaw, *supra* note 4, at 518 n.7 (citing instances of personal information being compromised in cybersecurity breaches as frequently as every three days).

39. WADE BAKER ET AL., VERIZON RISK TEAM, 2011 DATA BREACH INVESTIGATIONS REPORT 2 (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf.

40. *Id*. at 13 (illustrating breaches in several industry groups, including manufacturing, tech services, business services, media, and transportation).

41. *See id.* (showing the distribution of data breaches across industries). This report

Investigation (FBI) has also released a study showing that incidences of cybercrime continue to climb steadily.[42]

Given the modern technological nature of electronic data storage, the history of data security breaches spans a relatively short period of time.[43] Some of the most notable and severe security breaches in history include breaches at the TJX Company, exposing 95 million customers' credit and debit card account numbers;[44] Heartland Payment Systems, exposing 130 million payment card numbers;[45] TD Ameritrade, exposing six million files of customer contact information;[46] The Gap retail store, exposing private information of 800,000 job applicants;[47] and CitiGroup, exposing 210,000 customers' accounts.[48] The largest-ever reported breach occurred at Sony, where a breach revealed 144 million customers' confidential account data and credit and debit card numbers.[49] This trend has produced a burgeoning area of law that only promises to grow and evolve in coming years as an increasing volume of cybersecurity cases are litigated.

In light of the increasing threat to Americans concerning personal data loss and identity theft resulting from electronic security breaches, Congress—as well as numerous state legislatures—has taken action to implement a range of laws to remedy the growing problem. Some of these laws are designed to deter the crime of identity theft generally.[50] Other

---

observed that a change is underway, and that unlike in previous years in which ninety percent or more of records lost were derived from financial services targets, there is a trend to a more even distribution, presenting an expanded threat to other industries. *Id.*

42. *See* INTERNET CRIME COMPLAINT CTR., 2011 INTERNET CRIME REPORT 14 (2011), *available at* http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf (revealing an increase in reported cybercrimes from 16,838 in 2000 to 315,246 in 2011); *see also* Siobhan Gorman & Evan Perez, *FBI Probes Hack at Citibank*, WALL ST. J., Dec. 22, 2009, at A1.

43. *See Chronology of Data Breaches*, *supra* note 15 (compiling a list of data breach incidents since 2005).

44. *See* Jaikumar Vijayan, *Scope of TJX Data Breach Doubles: 94M Cards Now Said To Be Affected*, COMPUTERWORLD (Oct. 24, 2007, 12:00 PM), http://www.computerworld.com/s/article/9043944/Scope_of_TJX_data_breach_doubles_94M_cards_now_said_to_be_affected (explaining that the revelation of the doubling of the previously believed number makes this among the largest exposures of credit card numbers in history).

45. *See* Jessica Silver-Greenberg & Nelson D. Schwartz, *MasterCard and Visa Investigate Data Breach*, N.Y. TIMES (Mar. 30, 2012), http://www.nytimes.com/2012/03/31/business/mastercard-and-visa-look-into-possible-attack.html (reporting that the sophistication of hacking attacks on electronic financial data is increasing).

46. Sharon Gaudin, *Hacker Gained Access to Data on Millions of TD Ameritrade Customers*, INFORMATIONWEEK (Sept. 14, 2007, 1:46 PM), http://www.informationweek.com/news/201806604.

47. Sharon Gaudin, *Theft of Gap Laptop Puts 800,000 Job Applicants at Risk*, INFORMATIONWEEK (Oct. 1, 2007, 1:21 PM), http://www.informationweek.com/news/202103785.

48. Andy Greenberg, *Citibank Reveals One Percent of Credit Card Accounts Exposed in Hacker Intrusion*, FORBES (June 9, 2011, 10:00 AM), http://www.forbes.com/sites/andygreenberg/2011/06/09/citibank-reveals-one-percent-of-all-accounts-exposed-in-hack.

49. Deverich, *supra* note 5, at 27.

50. *See, e.g.*, *The Identity Theft Protection Act of 2000: Hearing on H.R. 4311*

laws require notification and public disclosure of data security breaches involving personal information.[51] While broader data security proposals have been introduced in Congress, federal legislators have largely allowed these bills to languish and have thus far failed to enact comprehensive data security legislation.[52]

While the enactment of state and federal legislation represents positive initial steps toward protecting against data breaches and identity theft, more comprehensive federal legislation is necessary to protect consumers from cybersecurity threats. Given the inconsistency of courts' willingness to recognize the increased risk of identity theft that data breaches pose, plaintiffs have faced an uphill battle finding relief through civil ligation.[53] Unless courts are successful in reducing the risk of loss to consumers by recognizing the costs associated with data loss and credit monitoring as sufficient to support standing, statutory means may be the only route to protect consumers by creating a statutory cause of action for victims. A move in this direction has already begun on the state level, as Hawaii considered a bill in 2011 that would authorize any person to sue who is a victim of a data security breach that creates a risk of harm by identity theft.[54]

However, as the state and federal law currently stands, these measures fall short of helping individuals who have been affected by a failure of data security and resulting identity theft.[55] Resolving the split among the Third,

---

Before the H. Comm. on Banking & Fin. Servs., 106th Cong. 106–13 (2000) (statement of Betsy Broder, Assistant Director for the Division of Planning and Information of the Bureau of Consumer Protection, Federal Trade Commission) (describing the Identity Theft and Assumption Deterrence Act's purpose of aiding law enforcement and preventing identity theft before it occurs). In 1998 Congress enacted the Identity Theft and Assumption Deterrence Act, making identity theft a federal crime. *See* Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028 (2006)).

51. In 2002, California was among the first states to enact a data breach security law, passing S.B. 1386, the first legislation requiring entities to notify an individual of any unauthorized acquisition of the individual's personal information. *See* CAL. CIV. CODE §§ 1798.29, 1798.80–.84 (West 2009). Today forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have all enacted legislation requiring notification of security breaches involving personal information. *See State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last updated Aug. 20, 2012) (reporting that the only states that have not yet enacted data security breach legislation are Alabama, Kentucky, New Mexico, and South Dakota).

52. *See* Julie A. Heitzenrater, Note, *Data Breach Notification Legislation: Recent Developments*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 661, 662–63 (2008) (asserting that Congress has failed to pass any unifying data breach legislation, leaving a "patchwork of state laws").

53. *See* Timothy H. Madden, *Data Breach Class Action Litigation—A Tough Road for Plaintiffs*, BOS. B.J., Fall 2011, at 27, 27–28 (explaining the reluctance of courts to allow data breach cases to proceed past the earliest stages of litigation).

54. S.B. 728, 26th Leg., Reg. Sess. (Haw. 2011).

55. *See* Rancourt, *supra* note 2, at 201–05 (discussing the inadequacies of current federal cybersecurity legislation).

Seventh, and Ninth Circuits in favor of permitting standing will best serve the interests of consumers by deterring risky data storage practices and minimizing the risk of greater economic loss as a result of identity theft.[56]

B. Article III Standing Requirements and Injury-in-Fact

Although the Constitution does not explicitly describe the standing doctrine, the Supreme Court has interpreted Article III's case-or-controversy requirement as a requirement for the plaintiff to prove standing.[57] For a federal court to exert jurisdiction over a particular case, one plaintiff must prove standing for the relief that the plaintiff seeks.[58] If a plaintiff fails to meet this requirement, the federal court must dismiss a case without deciding the merits.[59]

Under Article III, section 2 of the Constitution, federal judicial power is limited to resolution of "cases" and "controversies."[60] This standing requirement is one of the Court's several justiciability doctrines, which also include ripeness, mootness, political questions, and abstention.[61] The requirements of the standing doctrine are: (1) the plaintiff must have suffered injury-in-fact; (2) the plaintiff's injury must be fairly traceable to the actions of the defendant; and (3) the relief requested in the suit must redress the plaintiff's injury.[62] In addition to requirements of causation and redressability, which are not explored in detail here, a plaintiff must show "injury-in-fact," which is central to the discussion of data breach standing and is defined as "invasion of a legally protected interest."[63] This injury must be "concrete and particularized," "actual or imminent," and not "conjectural or hypothetical."[64] This limitation on the power of the federal

---

56. *See* Shaw, *supra* note 4, at 562 (suggesting that the adoption of comprehensive cybersecurity legislation will protect consumers by increasing the risk of liability for data storing companies and reducing the overall number of data breaches).

57. Bradford Mank, *Standing and Statistical Persons: A Risk-Based Approach to Standing*, 36 ECOLOGY L.Q. 665, 673 (2009) (noting that at least since *Stark* was decided, the Supreme Court has required Article III standing); *see also* Stark v. Wickard, 321 U.S. 288, 310 (1944) (stating for the first time the Article III standing requirements).

58. Mank, *supra* note 57, at 673.

59. *Id.*

60. U.S. CONST. art. III, § 2.

61. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 2.3, at 49–50 (4th ed. 2011) (outlining the several principles of justiciability that limit federal judicial power); *see also* Allen v. Wright, 468 U.S. 737, 750 (1984) (explaining that these doctrines reflect a concern about how to limit the role that courts have in a democratic society).

62. *See Allen*, 468 U.S. at 751 (reviewing the Supreme Court's standing jurisprudence). *See generally* Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459 (2008) (discussing the essential elements of the Article III standing requirements and their relative functions).

63. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (holding that the plaintiff lacked standing to challenge environmental regulations).

64. *Id.* (internal quotation marks omitted).

judiciary is fundamental to maintaining the appropriate separation of powers.[65]

Because the term "standing" embodies both constitutional requirements and prudential considerations,[66] it is not always clear in Supreme Court opinions whether Article III requires particular features of the standing doctrine or whether the Court itself has adopted these requirements.[67] Despite this uncertainty, the Supreme Court has established that at an "irreducible minimum,"[68] Article III standing requires that the party who seeks the court's action must "show that he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant."[69]

Injury-in-fact has been defined expansively to include injuries even to spiritual and aesthetic interests, in addition to mere economic and physical interests.[70] A plaintiff must also show that this factual injury is fairly traceable to the actions of the defendant,[71] and that it will likely be "redressed by a favorable decision."[72] The Supreme Court has applied the standing doctrine to serve several separation-of-powers functions for the courts, including hearing only cases with sufficient adversity capable of judicial resolution,[73] avoiding political questions better left to the political branches, and limiting use of citizen suits.[74]

One scholar notes that the standing doctrine is "notoriously difficult" to interpret and apply, observing that "lower courts resolving standing questions have produced contradictory results: cases with essentially the same facts come out in wildly different ways" and that "[s]uch unpredictability has generated extensive controversy."[75] With a lack of

---

65. *See Allen*, 468 U.S. at 752 (asserting that Article III standing is built on "a single basic idea—the idea of separation of powers"). *See generally* F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 56–65 (2012) (discussing the origins of Article III standing).

66. *See* Warth v. Seldin, 422 U.S. 490, 498 (1975) (explaining that the inquiry made in a standing analysis includes both constitutional and prudential limitations).

67. *See* Flast v. Cohen, 392 U.S. 83, 92–93 (1968) (articulating the confusion that developed in light of the Court's decision in Frothingham v. Mellon, 288 F. 252 (D.C. Cir. 1923), over whether the Court's holding was compelled by the Constitution).

68. *See* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 472 (1982) (delineating the Supreme Court's interpretation of the limitations on judicial power).

69. *Id.* (quoting Gladstone, Realtors v. Village of Bellwood, 441 U.S. 91, 99 (1979)).

70. Hessick, *supra* note 65, at 57 (noting the broad bounds of how injury is defined).

71. Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (delineating the causal connection requirement).

72. *Id.* (quoting Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 38 (1976)).

73. *See* Elliott, *supra* note 62, at 510–11 (arguing that the complexity of current doctrine is not needed to ensure that cases are "concretely adverse").

74. *See* United States v. Nixon, 418 U.S. 683, 697 (1974) (determining justiciability on the basis of sufficient adversity); Coleman v. Miller, 307 U.S. 433, 445–46, 458–59 (1939) (discussing the nonjusticiability of political questions and citizen suits).

75. *See* Elliott, *supra* note 62, at 466.

clear definitions to guide the application of the standing doctrine, courts often erroneously apply the doctrine as a decision on the merits under the pretense of a jurisdictional inquiry.[76]

Several leading cases, particularly *Whitmore v. Arkansas*,[77] *Lujan*, and *City of Los Angeles v. Lyons*,[78] serve to delineate the modern Court's interpretation of Article III standing requirements and are frequently cited by the lower courts. In *Whitmore*, the Court addressed the question of whether one death row inmate may bring a suit on behalf of another, ruling that the inmate lacked standing for failure to show injury-in-fact.[79] The Court held that that injury must be concrete in "both a qualitative and temporal sense."[80] The complainant must allege an injury to himself that is "distinct and palpable," as opposed to merely "[a]bstract."[81] Importantly, the Court in *Whitmore* noted that the "threshold inquiry into standing 'in no way depends on the merits of the [plaintiff's claim].'"[82]

Building on *Whitmore*, the Court in *Lujan* found that members of environmental groups who asserted injury due to lack of opportunity to observe endangered species did not show an injury which would be redressable as a result of their suit challenging a regulation of the Secretary of the Interior.[83] Not only did the Court hold that the groups did not make a claim of a harm that was redressable, the Court further held that the damage to a species as a product of government action did not suffice as an imminent harm to the plaintiffs that was sufficient for standing.[84] While this case dealt with standing in a challenge to government action—a context which is applicable to the original separation of powers purpose of the Article III standing requirement—courts erroneously use *Lujan* as a standard for measuring standing in a range of factual scenarios which do not serve the intent of the doctrine.[85] In *Lyons*, a case brought by a plaintiff who feared a future harm by the police force in Los Angeles, the Court again denied standing, emphasizing that cases will be dismissed in

---

76. *See id.* (citing Mark V. Tushnet, *The New Law of Standing: A Plea for Abandonment*, 62 CORNELL L. REV. 663, 663 (1977)) (noting various criticisms to the standing doctrine).

77. 495 U.S. 149 (1990).

78. 461 U.S. 95 (1983).

79. *Whitmore*, 495 U.S. at 156.

80. *Id.* at 155.

81. *Id.* (quoting O'Shea v. Littleton, 414 U.S. 488, 494 (1974)).

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

83. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 570–71 (1992) (declining to find a redressable injury where endangered species were threatened by projects in foreign countries partially funded by the Agency for International Development).

84. *See id.* at 564 (finding that past activity and future, but unplanned, intent were insufficient to constitute an injury).

85. *See, e.g.*, City of Los Angeles v. Lyons, 461 U.S. 95, 107 n.8 (1983) (observing that emotional trauma is relevant in determining standing but insufficient to constitute the basis for standing).

circumstances where the alleged future harm is not "real and immediate."[86]

In a line of recent cases, however, the Court has expanded plaintiffs' ability to reach the merits of their cases in situations involving emotional distress and a heightened risk of injury or fear. Among the most notable was the Supreme Court case *Doe v. Chao*,[87] in which the plaintiff sued the Department of Labor after it exposed his social security number beyond the limits of the Privacy Act.[88] The plaintiff alleged that he suffered emotional distress as a result of the exposure of his private information.[89] The Court applied a seemingly lower bar than in *Lujan*, acknowledging that a plaintiff who was "torn . . . all to pieces" and was "greatly concerned and worried because" of the potentially "devastating consequences"[90] of the exposure of his social security number had no cause of action under the Privacy Act, but nonetheless had standing under Article III.[91]

Lower courts have followed the *Chao* Court, conferring standing for plaintiffs who have suffered an increased risk of harm by the actions of the defendant. For example, in *Denney v. Deutsche Bank AG*,[92] the court observed, "injury-in-fact may simply be the fear or anxiety of future harm."[93] The *Denney* court further observed that the risk of future harm might also involve "economic costs, such as medical monitoring and preventative steps; but aesthetic, emotional or psychological harms also suffice for standing purposes."[94] Cases like *Denney* reflect a broadening of the Article III standing requirement to include emotional distress and anxiety.[95]

C. Lower Court Decisions and the Initial Trend Toward Denying Standing in Data Breach Cases

A survey of district court rulings in data breach cases reveals a history of inconsistent outcomes, but most courts support the conclusion that plaintiffs whose data has been breached, but not yet misused, have not suffered sufficient injury-in-fact to satisfy the standing requirements under

86. *Id.* at 110.
87. 540 U.S. 614 (2004).
88. *Id.* at 617.
89. *Id.*
90. *Id.* at 641 (Ginsburg, J., dissenting).
91. *See id.* at 624–25 (majority opinion) ("[A]n individual subjected to an adverse effect has injury enough to open the courthouse door, but without more has no cause of action for damages under the Privacy Act.").
92. 443 F.3d 253 (2d Cir. 2006).
93. *Id.* at 264.
94. *Id.* at 265.
95. *See, e.g.*, McLoughlin v. People's United Bank, Inc., No. 3:08-CV-00944, 2009 WL 2843269, at *2–4 (D. Conn. Aug. 31, 2009) (deciding that the plaintiffs had standing "where the plaintiffs' personal information [wa]s missing, ha[d] not yet been misused, but where the plaintiffs fear[ed] that it w[ould] be used improperly and to their financial detriment").

Article III.

In *Giordano v. Wachovia Securities, LLC*,[96] a bank customer opened a retirement account, providing the bank with her name, address, and social security number.[97] This data was later printed out as part of a report containing financial information about tens of thousands of customers, and was subsequently lost.[98] Because the customer did not suffer any actual or attempted identity theft, the court in *Giordano* held that the customer lacked standing to bring a claim on the basis of a risk of future identity theft.[99] The court determined that the customer lacked constitutional standing because she had failed to show that she suffered an injury-in-fact that was either "actual or imminent."[100] The court reasoned that the customer's allegations that, as a result of the corporation's actions, she would incur the costs of obtaining credit-monitoring services to prevent identity theft simply did not rise to the level of creating a concrete and particularized injury because such claims, at most, were speculative and involved merely hypothetical future injuries.[101]

The case *Bell v. Acxiom Corp.*[102] involved a corporation that specialized in storing personal and financial data for its corporate clients, whose computer database was compromised and client files were exposed.[103] A client filed a class action suit seeking damages and injunctive relief alleging that the security failure violated her privacy and left her at a risk of receiving junk mail and falling victim to identity theft.[104] The court granted a motion to dismiss, finding that the claim was not justiciable for lack of standing.[105] The court pointed out that "[a]ssertions of potential future injury" do not qualify as injury-in-fact, and a threatened injury must be certainly impending to constitute injury-in-fact.[106] The court added that while there had been numerous lawsuits alleging an increased risk of identity theft, no court had considered mere risk to be damage, and that only when the plaintiff had actually been the victim of identity theft had the courts found that there were cognizable injury and damages.[107]

The court in *Key v. DSW Inc.*[108] similarly held that a customer whose

96. No. 06-476, 2006 WL 2177036 (D.N.J. July 31, 2006).
97. *Id.* at *1.
98. *See id.* (noting that the report was lost in transit after being mailed with UPS).
99. *See id.* at *4 (reiterating that "[a] complaint alleging the mere potential for an injury does not satisfy Plaintiff's burden to prove standing").
100. *Id.*
101. *Id.*
102. No. 4:06cv00485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006).
103. *Id.* at *1.
104. *Id.*
105. *Id.* at *2–3.
106. *Id.* at *2.
107. *Id.*
108. 454 F. Supp. 2d 684 (S.D. Ohio 2006).

personal information had been compromised did not have standing to sue for future damages on the basis of an increased risk of identity theft.[109] The court observed that many jurisdictions embrace the rule that an alleged increase in risk of future injury cannot be considered an "actual or imminent" injury.[110] Thus, these courts have denied standing, or granted summary judgment for failure to establish damages, in negligence and breach of confidentiality claims brought in response to unlawful third-party access to secure data from a financial institution.[111] The court also noted that a lack of answers to the simple questions concerning who would cause harm to the customer, when it could occur, and how extensive the injury would be, illustrated the "indefinite and speculative" nature of the plaintiff's alleged injury.[112] In sum, the court reiterated that the customer's claims were based on little more than speculation that she would be the victim of wrongdoing at an unidentified point in the future.[113]

While these cases represent a larger trend toward denying standing among the lower courts, other courts have acknowledged standing, especially in the years since the 2007 *Pisciotta* decision in the Seventh Circuit.[114]

D. The New Circuit Split

The circuit courts have only recently begun to rule on the question of standing in data breach cases. The Seventh Circuit addressed the issue of standing in a data breach case as a matter of first impression in 2007,[115] followed by the Ninth Circuit in 2010[116] and the Third Circuit in 2011.[117] Reflecting the unsettled nature of cybersecurity law and the diverging outcomes in the lower courts, the issue of standing in data security breaches at the appellate level resulted in a circuit split.

The Seventh Circuit in *Pisciotta* rejected the trend of lower courts and charted a new course by recognizing standing for victims of data breaches, even when the plaintiffs' injuries were limited merely to the increased risk

---

109. *See id.* at 685 (holding that the plaintiff did not have standing because she failed to demonstrate that she suffered an injury-in-fact).
110. *Id.* at 689.
111. *Id.*
112. *Id.* at 690.
113. *Id.*
114. *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1051 (E.D. Mo. 2009) (noting that subsequent to *Pisciotta*, district courts have "consistently" upheld standing for increased risk of identity theft).
115. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634–35, 637 (7th Cir. 2007) (upholding the plaintiffs' claim as justiciable but finding that credit-monitoring costs were non-compensable damages in what was a "novel question of state law").
116. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
117. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

of identity theft.[118] The plaintiffs in *Pisciotta* brought a class action suit against a bank that failed to adequately secure the plaintiffs' online financial information, which was compromised when a third-party hacker gained access to the bank's database.[119] The *Pisciotta* court proposed an alternative analysis, referencing in footnotes several areas of tort law that support the notion that conferring standing should be appropriate for this class of plaintiffs.[120]

The *Pisciotta* ruling marked a turning point, where lower courts began increasingly to recognize standing for data breach victims. In *McLoughlin v. People's United Bank, Inc.*,[121] the U.S. District Court for the District of Connecticut ruled that plaintiffs had standing to sue where a bank lost up to ten unencrypted tapes with names, social security numbers, and bank account information.[122] The court found that the plaintiffs' mere fear of harm in the future was sufficient for standing and noted that the U.S. Court of Appeals for the Second Circuit standard for an injury-in-fact consists of as little as "simply . . . the fear or anxiety of future harm."[123] Likewise, the U.S. District Court for the Southern District of New York in *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*[124] found that an employee alleged adequate injury-in-fact for standing purposes when a laptop containing his personal information was stolen from his employer, but the court found that the employee could not sustain a claim under New York law for negligence or breach of fiduciary duty.[125] Although the lower court decisions show the weight of the authority largely on the side of denying standing, a minority of courts have begun to recognize standing, mostly in the wake of *Pisciotta*.[126]

A few years later, the Ninth Circuit in *Krottner* adopted and expanded the logic used in *Pisciotta*, finding that an act that harms the plaintiff only by increasing the risk of future harm to the plaintiff is enough to confer standing.[127] The claim in *Krottner* was based upon an allegation of

---

118. *See Pisciotta*, 499 F.3d at 634 (rejecting the notion that courts do not have subject matter jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing).

119. *Id.* at 631 (detailing the plaintiff's allegations).

120. *Id.* at 634 nn.3–4 (analogizing to an exposure to a toxic substances case and a defective medical equipment case).

121. No. 3:08-cv-00944, 2009 WL 2843269 (D. Conn. Aug. 31, 2009).

122. *See id.* at *1, *4 (concluding that the court had subject matter jurisdiction based on a standing analysis).

123. *Id.* at *4.

124. 580 F. Supp. 2d 273 (S.D.N.Y. 2008).

125. *Id.* at 276, 280, 282–83.

126. Deverich, *supra* note 5, at 28 (observing that since the ruling in *Pisciotta*, some courts have found that increased risk of identity theft is sufficient for standing).

127. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (ruling that the plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data").

increased risk of future identify theft stemming from a stolen laptop from a Starbucks coffee shop containing the names, social security numbers, and addresses of nearly one hundred thousand employees in an unencrypted file.[128] The court again upheld the notion that when a data breach plaintiff alleges that an act increased his risk of future harm by identity theft, this constitutes an injury-in-fact sufficient to satisfy the requirements of Article III.[129]

The recent circuit split was established in the December 2011 decision in *Reilly*, when the Third Circuit broke from the decisions of its sister courts in the Seventh and Ninth Circuits and denied standing for data breach victims based on the injury-in-fact requirement.[130] In *Reilly*, law firm employees brought a class action suit against a payroll-processing firm for alleged negligence in a breach of confidential personal data.[131] The *Reilly* court held that when plaintiffs fail to allege that there is actual misuse of the compromised data, there is neither a "concrete and particularized" injury, nor a threat of harm that is "certainly impending."[132] *Reilly* ruled that even expenditures made by victims to monitor credit information did not confer standing, and that these costs, which were meant to ease the fear of future third-party misuse of their information, are based on an injury that is too "speculative" and "hypothetical."[133]

To justify this holding, the Third Circuit went to great lengths to distinguish data breach plaintiffs from plaintiffs in various other factual scenarios where the law readily recognizes standing for an increased risk of harm, or for the costs of prophylactic monitoring services to detect and prevent future harm.[134] Although the court's vociferous refusal to acknowledge plaintiff's standing did not permit the case to proceed to the merits, subsequent charges filed separately by the Federal Trade Commission (FTC) belied the reality that Ceridian's failure to secure its customers' personal and financial data had wrought serious harm requiring a legal remedy.[135] The FTC's claim set out charges that Ceridian

128. *Id.* at 1140.
129. *Id.* at 1143.
130. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) ("[A]llegations of an increased risk of identity theft as a result of the security breach are hypothetical, future injuries, and are therefore insufficient to establish standing."), *cert. denied*, 132 S. Ct. 2395 (2012).
131. *See id.* at 40 (noting that 27,000 employees at 900 companies had personal and financial information exposed).
132. *See id.* at 43, 46 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 595 n.2 (1992)); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007).
133. *Reilly*, 664 F.3d at 46.
134. *See id.* at 44–46 (seeking to distance data breach claims from toxic exposure, faulty medical device, and environmental claims involving latent harm, asserting erroneously that in data breach scenarios there is no actual quantifiable injury that occurs, and that because human bodily health concerns are not implicated, standing should not be granted).
135. *See FTC Settles Charges Against Two Companies That Allegedly Failed to Protect*

misrepresented the integrity of its security measures and failed to adequately protect its network from "reasonably foreseeable attacks," enabling a hacker to breach one of Ceridian's electronic payroll processing applications and compromising the personal information of thousands of customers.[136] The FTC's resulting Consent Agreement with Ceridian mandated that the company refrain from misleading data security claims, implement a comprehensive security program designed to better protect the confidentiality and integrity of personal information collected by consumers, and submit to biennial third-party security audits for a twenty-year period.[137]

On May 14, 2012 the Supreme Court denied plaintiff Reilly's petition for certiorari,[138] delaying resolution of the circuit split, perhaps for the purpose of allowing data breach litigation to achieve broader consideration by the federal circuit courts. Indeed, since the Supreme Court denied certiorari in *Reilly*, this standing issue continues to percolate through the courts, most recently reaching the U.S. Circuit Court of Appeals for the First Circuit in *Katz v. Pershing, LLC*.[139] In that case, the customer of a financial data services company alleged a lack of adequate data security protocols, placing the plaintiff at an increased risk of harm due to the loss of her secure personal data.[140] The court denied the plaintiff standing, but noted the lack of an important common denominator with *Pisciotta*, *Krottner*, and *Reilly*.[141] In each of those cases the claims arose as a consequence of the actual misappropriation of sensitive personal data by a third party. In *Katz*, however, the plaintiff merely claimed a risk of future harm due to a perceived weakness in data security, not that the security deficiency had resulted in exposure to an unauthorized person.[142] The court held that the lack of an actual data breach was a "fatal" omission for the standing analysis, suggesting that had a hacker actually misappropriated her data she would have satisfied "Article III's requirement of actual or impending injury."[143] The *Katz* decision, while noting the "disarray" among the circuit courts concerning standing on the basis of increased risk in data breach cases, may indicate a movement toward the standard upheld

---

Sensitive Employee Data, FED. TRADE COMM'N (May 3, 2011), http://www.ftc.gov/opa/2011/05/ceridianlookout.shtm (describing the charges against Ceridian for "fail[ure] to employ reasonable and appropriate security measures to protect" large amounts of sensitive data about its business customers in violation of federal law).

136. *Id.*

137. *See* Ceridian Corp., 151 F.T.C. 514, 520–23 (2011) (detailing the terms of the FTC Consent Agreement).

138. Reilly v. Ceridian Corp., 132 S. Ct. 2395 (2012).

139. 672 F.3d 64 (1st Cir. 2012).

140. *Id.* at 70.

141. *Id.* at 80.

142. *Id.*

143. *Id.*

in *Pisciotta* and *Krottner*, and a repudiation of *Reilly*.[144]

II. DATA BREACH PLAINTIFFS SHOULD NOT BE TURNED AWAY AT THE COURTHOUSE STEPS

A. The Supreme Court's Standing Doctrine Permits Justiciability of Data Breach Victims' Claims

The original purpose of the constitutional standing requirement was to ensure the separation of powers delineated by the Constitution.[145] The standing doctrine also encompasses several judicially self-imposed prudential standing requirements to limit federal jurisdiction.[146] These include the "general prohibition on a litigant's raising another person's legal rights, the rule barring adjudication of generalized grievances more appropriately addressed in the representative branches, and the requirement that a plaintiff's complaint fall within the zone of interests protected by the law invoked."[147]

The standing requirement was also originally intended to ensure litigants are persons likely to be most directly affected by a court's ruling.[148] Guided by this goal of the standing doctrine, the Court rejects claims that are merely "a vehicle for the vindication of the value interests of concerned bystanders."[149] Expounding on this rationale, the Court has said: "The exercise of judicial power, which can so profoundly affect the lives, liberty, and property of those to whom it extends, is therefore restricted to litigants who can show 'injury in fact' resulting from the action which they seek to have the court adjudicate."[150]

Similarly, a fundamental purpose of the standing doctrine is to prevent citizens from bringing suits predicated on abstract injuries such as violations of generalized rights by government action.[151] The Supreme Court has repeatedly rejected claims of standing based on "the generalized

144. *See id.* (noting the outcomes in *Reilly*, *Krottner*, and *Pisciotta*).

145. *See* Allen v. Wright, 468 U.S. 737, 752 (1984) ("[T]he law of Art. III standing is built on a single basic idea—the idea of separation of powers.").

146. *Id.* at 751.

147. *Id.*

148. *See* United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S. 669, 687 (1973) (explaining that to demonstrate standing a plaintiff must show that he or she has "a direct stake in the controversy" and is not just a concerned third party).

149. *Id.*

150. Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 473 (1982).

151. *See id.* at 482–83 (explaining the Court's decision to reject claims of standing based solely on the fact that citizens are generally unhappy with government action, and stating that allowing citizens to have federal standing in these situations would mean "to employ a federal court as a forum in which to air . . . generalized grievances about the conduct of government" (quoting Flast v. Cohen, 392 U.S. 83, 106 (1968))).

interest of all citizens."[152]

Application of the standing doctrine to modern cybersecurity cases reveals that denying standing to victims of data exposure does not even remotely serve the original purposes of this justiciability requirement. This survey of Supreme Court jurisprudence shows that the essence of the Article III standing requirements boils down to ensuring cases have concrete adversity that is capable of judicial resolution, avoiding questions best answered by the political branches of government, and avoiding citizen suits.[153] None of these foundational concerns are at play in cases like *Pisciotta*, *Krottner*, and *Reilly*. The actions individuals must take following a breach of their personal information, such as buying identity theft insurance, protecting their finances with credit-monitoring services, replacing credit cards, and ordering new checks, are all concrete, reasonable expenses, and economic losses resulting from the alleged negligence of the data storage entity.[154] It is therefore possible to restore the victim's losses by covering these costs. Thus, data breach cases easily hurdle the requirement that a claim include a concrete adversity that is redressable. Further, data breach cases involve neither political questions nor taxpayers seeking to enforce statutes, and therefore they do not threaten to violate the political question or "citizen suit" justiciability principles.

Courts that fail to permit standing in data security cases have strayed too far from the Constitution's Article III justiciability requirements and set the threshold for injury-in-fact beyond what the Supreme Court's standing jurisprudence warrants, unjustly limiting plaintiffs' access to the courts.[155] Courts too often abuse the standing inquiry as an opportunity to avoid ruling on the merits, prematurely dismissing cases on jurisdictional grounds that they believe could not succeed on the merits.[156] While it can be difficult for plaintiffs to prove compensable damages in cybersecurity cases,[157] courts that doubt success on the merits but properly apply the standing doctrine would permit standing, and only dismiss a claim after the plaintiff has made his case.[158] Data breach cases present factual questions

---

152. *Id.* at 483 (quoting Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 217 (1974)).

153. *See supra* notes 73–74 and accompanying text.

154. These expenses are analogous to the expenditures made by plaintiffs in toxic exposure and defective medical device cases discussed *infra* Part II.B.

155. *See* Elliott, *supra* note 62, at 467 (asserting that the way courts apply the standing doctrine does not achieve the original goal of promoting separation of powers).

156. *See id.* at 466 (articulating the criticism that courts use the standing doctrine to decide cases on the merits under the "guise of a threshold jurisdictional inquiry").

157. *See* Rancourt, *supra* note 2, at 195 (describing how plaintiffs in data breach cases frequently struggle to quantify monetary losses and how courts take divergent approaches to the issue).

158. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639–40 (7th Cir. 2007) (recognizing the plaintiffs' ability to bring a claim for an increased risk of identity theft, but

concerning the nature and quality of the defendant's electronic security measures, and assessments of quantifiable measures of risk faced by the plaintiff; these questions are best resolved at trial and to do so they must survive the jurisdictional standing inquiry.

B. Application of Analogous "Latent Harm" Tort Law Principles to Standing in Data Breach Cases Compels a Finding of Article III Standing

The intractable split in the courts over standing in data security breaches can be resolved by applying a line of cases finding injury-in-fact in analogous situations where a defendant's actions increased the plaintiff's risk of future harm. These cases show by analogy that the fact that a plaintiff has suffered a breach of his or her data security, but has not experienced actual identity theft, should not bar standing to sue. Applying the principles upheld by courts in the cases below, courts should recognize plaintiff standing for the harm of increased risk of identity theft.

The court in *Pisciotta* acknowledged standing for the plaintiff with only modest support for doing so,[159] while the *Krottner* court extended the rationale for this holding with reference to courts that acknowledged an injury-in-fact in a variety of factual contexts.[160] *Reilly* by contrast, offers an extended yet flawed analysis in which the court endeavors to distinguish data breaches from all fact patterns in which courts recognize a present injury for a credible threat of future harm.[161] The *Reilly* court's two principle assertions—that in data breach cases no actual injury (or quantifiable risk of future harm) is present, and that standing for future injury must hinge on human bodily health concerns—are unpersuasive and contradict controlling tort principles.[162]

1. Toxic exposure

In toxic exposure cases, a plaintiff who has no current symptoms of a particular disease, but has reason to believe that he or she will become symptomatic with that disease at some point in the future as a direct result of a toxic environmental exposure, may bring a claim for damages to pay

---

dismissing the case on the merits for their inability to prove compensable damages).

159. *See id.* at 634 & nn.3–4 (citing authority in the footnotes without further explanation).

160. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (noting briefly how several courts have granted standing for future injury in environmental and medical-monitoring claims).

161. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 45–46 (3d Cir. 2011) (attempting to distinguish claims of latent harm, including environmental harm, toxic exposure, and defective medical device cases), *cert. denied*, 132 S. Ct. 2395 (2012).

162. *See id.* at 45 (distinguishing an injury suffered from a data breach from one suffered in a medical or environmental case because there is "no change in the status quo" and it does not implicate "human health concerns").

for preventative medical-monitoring care. For example, in *In re "Agent Orange" Product Liability Litigation*,[163] the court rejected the argument that "injury in fact means injury that is manifest, diagnosable or compensable."[164] There, Vietnam War veterans brought a toxic exposure claim against companies that manufactured the chemical defoliant Agent Orange.[165] Although many of the hundreds of thousands of soldiers who were exposed to the toxic chemical in the course of their service fell ill as a consequence of exposure, this class action was brought, in part, on behalf of "those individual veterans manifesting no symptoms of illness and disease at present, but at risk of genetic and somatic damage."[166] In other words, the suit was brought on behalf of those soldiers who had been exposed to the chemical but did not show outward signs of illness. The court in this case ruled that the "injury" to the asymptomatic plaintiffs occurred by their "at risk" status due to the chemical exposure.[167] The increased risk of future harm was effectively a present injury.[168]

This principle of increased risk as the foundation for a claim is directly applicable to plaintiffs like those in *Reilly*, *Pisciotta*, and *Krottner*, who have been subjected to a heightened risk of harm by the actions of the defendants who failed to properly secure their data. The defendant's argument in *Reilly* that the plaintiffs merely alleged a speculative or conjectural harm is the same made by the defendant chemical company in *"Agent Orange" Product Liability Litigation*.[169] This argument also wrongfully ignores the plaintiffs' heightened "at risk" status and should similarly be discarded.

---

163. 996 F.2d 1425 (2d Cir. 1993), *overruled in part on other grounds by* Syngenta Crop Prot., Inc. v. Henson, 537 U.S. 28 (2002).

164. *Id.* at 1434 (internal quotation marks omitted). In a notable 1997 toxic exposure case, however, the Supreme Court indicated that there are limits to the damages plaintiffs may recover when they are exposed to a toxic substance but remain asymptomatic. Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424 (1997). In *Metro-North*, a railroad employee brought an action under the Federal Employers' Liability Act (FELA), 45 U.S.C. § 51, alleging negligent infliction of emotional distress in connection with his exposure to asbestos. 521 U.S. at 427. Although much of the Court's analysis addressed whether exposure to asbestos dust constitutes a "physical impact" sufficient to support an emotional distress claim, the court also considered the bounds of tort liability for medical-monitoring costs. *Id.* at 438–44. The Court held that although plaintiffs have a recognized tort law cause of action to recover for medical-monitoring costs, this liability is not unqualified, and may be limited in a claim under FELA. *Id.* at 444.

165. *See "Agent Orange" Prod. Liab. Litig.*, 996 F.2d at 1428 (summarizing the protracted background of the litigation).

166. *Id.* at 1428, 1433 (internal quotation marks omitted).

167. *Id.* at 1434.

168. *Id.* at 1433–34.

169. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 44–45 (3d Cir. 2011) (labeling the plaintiffs' increased risk of injury too speculative and hypothetical), *cert. denied*, 132 S. Ct. 2395 (2012), *with "Agent Orange" Prod. Liab. Litig.*, 996 F.2d at 1434 (finding plaintiffs' risk of future harm due to chemical exposure sufficient injury to pursue a claim).

A similar analysis has been upheld in a variety of other toxic exposure scenarios, all of which exhibit a close analogy to the latent harm in the risk of identity theft. In *Duke Power Co. v. Carolina Environmental Study Group, Inc.*,[170] the Supreme Court upheld standing for plaintiffs opposing the construction of a nuclear power plant near their homes.[171] The plaintiffs had not yet suffered any physical injury as a result of exposure to nuclear emissions—their claim was instead based on the mere possibility that they may be exposed to nuclear contamination in the future and that they would be subject to the "present fear and apprehension" regarding proximity of the plant.[172]

The reasoning in *Duke Power* mirrors the reasoning necessary to support standing for plaintiffs in data breach cases. Just as the plaintiffs in *Duke Power* had not suffered the actual toxicity of the power plant,[173] the victims in *Reilly* had not suffered actual identity theft, yet were still put at an increased risk of harm.[174] Further, the "present fear and apprehension" that supported a finding of standing in *Duke Power* is also relevant in that victims of data exposure may reasonably suffer fear and anxiety that severe consequences may result from identity theft, such as damaged credit and future inability to obtain a loan, and insecurity of financial accounts.[175] The Third Circuit's analysis in *Reilly* overlooks the fact that the present distress and fear a person suffers in anticipation of a future harm is a cognizable injury for standing purposes.[176]

The Third Circuit considered medical monitoring in *In re Paoli Railroad Yard PCB Litigation*,[177] holding that a cause of action for medical monitoring is cognizable in order to cover the cost of periodic medical examinations.[178] Like in the toxic exposure cases above, these medical evaluations were necessary to detect and prevent potentially latent diseases as a result of exposure to hazardous substances, in this case, toxic polychlorinated biphenyls (PCBs).[179] The court outlined the difference

---

170. 438 U.S. 59 (1978).
171. *Id.* at 67, 81.
172. *Id.* at 73.
173. *See id.* at 72–73 (characterizing the power plants as only "potentially dangerous" to the plaintiffs, putting them at a risk of future injury).
174. *See Reilly*, 664 F.3d at 40 (noting the plaintiffs' allegations of an increased risk of future identity theft).
175. Joshua R. Levenson, *Strength in Numbers: An Examination into the Liability of Corporate Entities for Consumer and Employee Data Breaches*, 19 U. FLA. J.L. & PUB. POL'Y 95, 112–13 (2008) (noting that financial losses due to identity theft affect victims in different ways including credit card disruptions, damaged credit ratings, harassment by debt collectors, rejected applications for loans and insurance, and other issues).
176. *See supra* notes 87–91 and accompanying text.
177. 916 F.2d 829 (3d Cir. 1990).
178. *See id.* at 852 (interpreting Pennsylvania law and speculating that the Supreme Court of Pennsylvania would recognize such a cause of action).
179. *See id.* at 835–36 (delineating the plaintiffs' claims of exposure to abnormally high

between medical-monitoring claims and damages claims involving an increased risk of harm without a present physical injury.[180]

The Third Circuit in *Paoli* considered medical monitoring a tort in and of itself, as opposed to a remedy for the underlying tort of exposure to an increased risk of future harm.[181] The court contrasted a claim for medical monitoring to a claim for damages based on the enhanced risk, stating: "an action for medical monitoring seeks to recover only the quantifiable costs of periodic medical examinations necessary to detect the onset of physical harm, whereas an enhanced risk claim seeks compensation for the anticipated harm itself, proportionately reduced to reflect the chance that it will not occur."[182]

This rationale is useful in an analysis of plaintiff standing in data security cases as well. Just as the costs of medical monitoring are independent of the potential future illness, credit-monitoring costs are distinguishable from whatever harm may occur in the future as a result of identity theft.[183] Such present, immediate costs must reasonably be considered concrete and particularized injuries worthy at least of standing, if not as compensable damages.

Although the *Reilly* court cites *Paoli* for ostensible support,[184] the *Paoli* decision in fact undermines the *Reilly* court's claim that standing should not be granted where outward injury is not present but looms in the future. The court in *Paoli* explained that people suffering only an "increased risk" of cell damage—not actual cell damage—have a present cause of action,[185] just as data breach plaintiffs suffer an increased risk of future injury. In either case, notwithstanding greater harm that may result in the future, when a defendant creates a risk of harm requiring monitoring costs, whether they are medical or financial costs, the damage has been done.

2. Defective medical devices

Injury-in-fact is also found, and medical-monitoring costs awarded, in

---

levels of PCB and resulting harm).

180. *See id.* at 850 (asserting that actions for medical monitoring seek to recover merely the costs of medical examinations necessary to detect the presence of physical harm, "whereas an enhanced risk claim seeks compensation for the anticipated harm itself").

181. *Id.* at 850–51.

182. *Id.* at 849–51.

183. *Id.* at 850; *see also* Johnson, *supra* note 36, at 122 (exploring the similarities between medical monitoring and credit monitoring).

184. Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) (citing *In re Paoli*, 916 F.2d at 851–52) (asserting that in toxic torts the damage has been done once contamination occurs and not once contamination causes illness), *cert. denied*, 132 S. Ct. 2395 (2012).

185. *See In re Paoli*, 916 F.2d at 852 (emphasizing that a plaintiff must suffer a "significantly increased risk" of serious disease as the result exposure to toxic materials and it is this "increased risk [that] makes periodic diagnostic medical examinations reasonably necessary").

cases where there is prospective harm in the potential failure of a defective medical device. In a U.S. Court of Appeals for the Sixth Circuit case, *Sutton v. St. Jude Medical S.C., Inc.*,[186] a class of plaintiffs who were implanted with a potentially faulty medical device during cardiac bypass surgery sued the hospital and device creator.[187] The plaintiffs' claim sought the imposition of a medical-monitoring fund for the patients who were put at an increased risk of health complications as a consequence of the defendant's actions.[188] This fund would cover the costs of tests and medical evaluations with the purpose of preventing future harm and discovering injury that may manifest itself in the future.[189] The court observed that tort plaintiffs have increasingly been awarded medical-monitoring costs in both toxic tort and product liability cases.[190] The court acknowledged standing under Article III and reasoned that medical-monitoring awards aid currently healthy plaintiffs who have been exposed to an increased risk of future harm to detect and treat any resulting harm at an early stage.[191] Further, the court rejected the notion that the "immediacy" of injury is necessarily required for standing—latent harm will suffice.[192] The court held that whether the plaintiff was likely to succeed on the merits was "not a proper consideration" in an inquiry about standing.[193] The holding in *Sutton* that plaintiffs who are at an increased risk of future harm and are subject to attendant monitoring costs have Article III standing to sue is a relatively recent but broadly accepted principle of law.[194]

The remedy of medical-monitoring costs perfectly parallels the costs incurred by plaintiffs in data breach cases for credit-monitoring costs: like periodic tests to evaluate the health of their body, credit monitoring serves

186. 419 F.3d 568 (6th Cir. 2005).
187. *Id.* at 569.
188. *Id.*
189. *Id.* at 569–70.
190. *See id.* at 571 (citing Arvin Maskin et al., *Medical Monitoring: A Viable Remedy for Deserving Plaintiffs or Tort Law's Most Expensive Consolation Prize?*, 27 WM. MITCHELL L. REV. 521, 522 (2000)).
191. *Id.* at 571.
192. *Id.* at 572. The court noted that in a previous case where medical monitoring was awarded, the monitoring was immediately necessary to prevent irreparable harm. *Id.* (citing Friends for All Children, Inc. v. Lockheed Aircraft Corp., 746 F.2d 816 (D.C. Cir. 1984)). In *Sutton*, however, it concluded that immediacy was not required. *Id.*
193. *Id.* at 574.
194. *See id.* at 571–75 (citing a multitude of defective medical device and product liability cases, e.g., Baur v. Veneman, 352 F.3d 625, 634 (2d Cir. 2003); Willett v. Baxter Int'l, Inc., 929 F.2d 1094 (5th Cir. 1991); Taylor v. Medtronics, Inc., 861 F.2d 980 (6th Cir. 1988); Harris v. Purdue Pharma, L.P., 218 F.R.D. 590, 595 (S.D. Ohio 2003)); *see also* Adam P. Joffee, Comment, *The Medical Monitoring Remedy: Ongoing Controversy and a Proposed Solution*, 84 CHI.-KENT L. REV. 663, 664 (2009) (observing that the American Law Institute (ALI) is set to endorse medical-monitoring awards in the Restatement (Third) of Torts).

to ensure the financial health of the plaintiffs.[195] Moreover, the court in *Sutton* stated that "there is something to be said for disease prevention, as opposed to disease treatment," opining that it was "both overly harsh and economically inefficient" to offer redress only after a plaintiff has experienced physical injury.[196] Prophylactic measures of credit monitoring to prevent financial harm to data breach plaintiffs will certainly reap benefits in the same way and will prevent larger economic losses.[197]

However, the court's holding in *Reilly* effectively forces plaintiffs to wait until their bank accounts have been raided and they have suffered the full consequences of identity theft to sue, instead of granting the plaintiffs the opportunity to seek available preventative measures.[198] The impact of following this path and failing to employ protective measures could be ruinous to a data breach victim's financial and emotional wellbeing.[199] One of the *Reilly* court's failures is its characterization of data breach plaintiffs' preventative credit-monitoring expenditures as "willingly incurred costs."[200] On the contrary, victims of data loss who spend resources to ensure the security of their finances do so prudently as a necessary measure to attenuate their increased vulnerability to fraud.[201] The expenses must be considered a real, present, and particularized injury sufficient for standing.

3. Environmental harm

The parallels between the risk of harm data breach plaintiffs face and the injury to plaintiffs in environmental harm cases is equally strong. In the Ninth Circuit environmental case *Central Delta Water Agency v. United States*,[202] the court recognized latent harm as a possible basis for a claim.[203] The court acknowledged that determining jurisdictional standing in the case required consideration of when a party may sue to prevent a future injury that it believes another's actions will cause.[204] The claim in *Delta Water*

195. There are many credit-monitoring services available to the general public. *See, e.g.*, *Credit Monitoring*, EXPERIAN, http://www.experian.com/consumer-products/credit-monitoring.html (last visited June 15, 2013).

196. *Sutton*, 419 F.3d at 575 (emphasis omitted).

197. *See* Johnson, *supra* note 36, at 113 (explaining that preventative measures can ensure against financial ruin and the inability to get credit or obtain employment).

198. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (denying standing based on credit-monitoring expenses), *cert. denied*, 132 S. Ct. 2395 (2012).

199. *See* Johnson, *supra* note 36, at 137 (referencing emotional distress, in addition to financial trouble, as a consequence of personal data exposure).

200. *See Reilly*, 664 F.3d at 46.

201. *See* Johnson, *supra* note 36, at 113 (describing how credit monitoring allows the victims of a data breach to take immediate measures in order to "avoid financial ruin").

202. 306 F.3d 938 (9th Cir. 2002).

203. *See id.* at 950 (explaining that "plaintiffs need not wait until the natural resources are despoiled before challenging the government action leading to the potential destruction").

204. *Id.* at 943.

was brought by California farmers against the U.S. Bureau of Reclamation, challenging a plan to release water from a reservoir into a river in California's Central Valley to comply with fish habitat restoration requirements.[205] The claim alleged that this release would create a substantial risk that the farmers' crops would not survive.[206] The plaintiffs claimed that the high salinity of the water would diminish their ability to grow crops because they used the water to irrigate their fields.[207] However, the plaintiffs had only been threatened with this injury, no crop loss had yet occurred.[208] The court held that plaintiffs need not establish that they in fact have standing, but only that there is a genuine question of material fact as to the standing elements, and further found that the plaintiffs had at the very least raised a material question of fact with respect to the issue of whether they suffer a substantial risk of harm as a result of the Bureau's policies.[209] Therefore, the court held that the alleged risk was sufficient to confer standing.[210]

Applied to data breach cases, such as *Reilly*, *Pisciotta*, and *Krottner*, this standard shows it is improper for a court to issue a dismissal for lack of standing when the judge must make a determination whether the future risk is great enough to amount to injury-in-fact. Because such inquiries in data breach cases are so factually driven—requiring an assessment of the adequacy of data security in place and the level of risk faced by the data breach victim[211]—dismissal for lack of standing cannot be appropriate where a plaintiff alleges a future threat of identity theft.

The *Village of Elk Grove Village v. Evans*[212] decision similarly supports the environmental claim analogy to data breach claims. There, municipal officials sued to prevent the Corps of Engineers from issuing a permit to construct a radio tower in a floodplain near the village.[213] The Seventh Circuit found standing because the village was in the path of a potential flood and "even a small probability of injury is sufficient to create a case or controversy."[214] This proposition—that even a small chance of harm that is

205. *Id.* at 945–46 (describing how the claims arose following passage of the Central Valley Project Improvement Act, Pub. L. No. 102-575, 106 Stat. 4600 (1992)).
206. *Id.* at 947.
207. *Id.*
208. *Id.*
209. *See id.* at 947, 950 (citing Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 104, 118 (1998)) (noting that the plaintiffs need only show that the facts alleged, if proved, would confer standing).
210. *Id.* at 950.
211. *See, e.g.*, McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944, 2009 WL 2843269, at *1, *3, *7 (D. Conn. Aug. 31, 2009) (noting that in a comparable Maine statute, the court required ascertainable loss of personal data to ensure that the alleged is palpable).
212. 997 F.2d 328 (7th Cir. 1993).
213. *Id.* at 328.
214. *Id.* at 329.

remediable by the court is injury-in-fact sufficient for standing—undermines the ruling in *Reilly* that the threat of identity theft is too "conjectural" and "hypothetical."[215] Applying the analysis employed in *Evans*, the inherent threat of harm to an individual who suffers the exposure of sensitive personal data exceeds this requirement, especially since the harm incident to identity theft can be mitigated.[216]

Other environmental cases support the same conclusion as well. The U.S. Court of Appeals for the District of Columbia Circuit in *Mountain States Legal Foundation v. Glickman*[217] held that an increased risk of wildfire as the result of certain logging practices constitutes injury-in-fact.[218] The U.S. Court of Appeals for the Fifth Circuit in *Sierra Club, Lone Star Chapter v. Cedar Point Oil Co.*[219] granted standing to environmentalists who anticipated the future pollution of a bay and did not require evidence of actual harm to a waterway, noting "[t]hat this injury is couched in terms of future impairment rather than past impairment is of no moment."[220]

Finally, in another key case involving future risk of waterway pollution, *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*,[221] an environmental advocacy group brought an action to prevent environmental damage.[222] Like the plaintiffs in data breach cases, the plaintiffs in *Friends of the Earth, Inc.* alleged an increased risk of future harm.[223] Ruling on the standing issue, the court concluded that the plaintiffs' reasonable fear and

---

215. Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

216. *See, e.g.*, James Graves, Comment, *"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Necessity of Measures to Avoid Identity Fraud After a Data Breach*, 16 RICH. J.L. & TECH., no. 1, 2009, at 48–49, http://law.richmond.edu/jolt/v16i1/article2.pdf (noting that credit-monitoring services frequently include identity theft insurance which will compensate victims for the costs of responding to identity theft); *see also* Elisabeth Goodridge, *Steps To Prevent Identity Theft, and What To Do if It Happens*, N.Y. TIMES (May 1, 2009), http://www.nytimes.com/2009/05/02/your-money/identity-theft/02Id theftprimer.html?pagewanted=all (suggesting that identity theft insurance can reassure those who have fallen victim to identify theft); Lynnette Khalfani-Cox, *Why Critics Are Wrong About Credit Monitoring Services*, DAILY FIN. (June 14, 2010), http://www.dailyfinance.com/2010/06/14/why-critics-are-wrong-about-credit -monitoring-services/ (asserting that even if credit monitoring does not prevent identity theft, it helps detect and deter fraudulent activity to minimize damage).

217. 92 F.3d 1228 (D.C. Cir. 1996).

218. *See id.* at 1234–35 (explaining that an "incremental risk is enough of a threat of injury" to allow plaintiff standing).

219. 73 F.3d 546 (5th Cir. 1996).

220. *Id.* at 556.

221. 204 F.3d 149 (4th Cir. 2000) (en banc).

222. *See id.* at 150 (detailing the plaintiffs' claims that the pollution adversely affects how they use the lake allegedly polluted by the defendants, such as by limiting the time spent swimming in it, causing them to limit the amount of fish they eat caught from the lake, and a hesitation to scuba dive in it because of the contamination).

223. *See id.* at 153, 156 (noting the potential for heavy metals and chemical pollution in local waterways).

concern about the potential effects of the polluting discharge, supported by objective evidence, directly affected the plaintiffs "recreational and economic interests" and that this type of "impact constitutes injury in fact."[224]

Evaluating claims by data breach victims in light of this line of "latent harm" environmental cases illustrates a willingness in courts to permit plaintiffs to sustain a claim for an increased risk of future harm. The rationale in these cases logically supports the notion that standing must be upheld in data breach cases and mutes arguments to the contrary.

C. The Economic Loss Rule Should Not Bar Recovery of Damages in Data Security Claims and Is Irrelevant to the Standing Analysis

The economic loss doctrine, also known as the economic loss rule, is a tort principle requiring courts to distinguish damages that are characterized as economic loss from non-economic damages.[225] Courts may consider the economic loss rule as a potential bar for plaintiffs seeking recovery for negligent loss of their secure personal information.[226] Under this doctrine, damages for non-economic losses are recoverable through tort law, while damages deemed to be purely economic loss, when not also involving personal injury or property damage, are recoverable only through contract law.[227] There is little consensus among the courts, however, on how these distinctions properly apply, and the rule is subject to myriad exceptions where certain purely economic damages are actionable in tort.[228] Exceptions permitting recovery of pure economic loss include negligent misrepresentation, breach of fiduciary duty, professional malpractice, nuisance, and defamation.[229]

---

224. *Id.* at 161.

225. *See* Ralph C. Anzivino, *The Economic Loss Doctrine: Distinguishing Economic Loss from Non-Economic Loss*, 91 MARQ. L. REV. 1081, 1081–82 (2008) (explaining that the distinction is important because economic damages can only be recovered through contract law but non-economic damages can be recovered under tort law).

226. *See* Krottner v. Starbucks Corp., 406 F. App'x 129, 132 (9th Cir. 2010) (raising the economic loss rule as a potential bar but declining to rule on the issue); *see also* Paul v. Providence Health Sys.-Or., 240 P.3d 1110, 1116 (Or. Ct. App. 2010) (ruling that data breach victims could not recover pure economic damages for expenses incurred by purchasing credit-monitoring services), *aff'd*, 273 P.3d 106 (Or. 2012).

227. *See* Anzivino, *supra* note 225, at 1081 (explaining that, under the economic loss doctrine, in most states a case may only advance as a contract case or a tort case, but not both); *see also* Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 381 (2006) ("[M]any jurisdictions do not allow plaintiffs to recover for economic losses absent any physical injury, under the economic loss doctrine.").

228. Anzivino, *supra* note 225, at 1081.

229. *See* Johnson, *supra* note 36, at 122 (discussing the "multitude of well-recognized exceptions" to the economic loss rule).

The intent of the economic loss doctrine is to encourage parties to regulate their economic relationships through contract law, by "limiting a plaintiff to contractual remedies for loss of the benefit of the bargain."[230] However, a number of data security laws provide that a waiver of an individual's rights in data security is contrary to public policy, and therefore void and unenforceable, meaning corporations and individuals are limited in their ability to contract around data security obligations.[231] Further, it is not practical for individual consumers and employees to bargain over data security contract provisions with each of the large corporations that collect and maintain their secure information in so many aspects of their lives.[232] Because the law frequently limits consumers' ability to enter contractual relationships with organizations concerning their data security rights, and because it is not practical for them to do so, it would be nonsensical for the economic loss rule to bar plaintiffs' claims of damages for exposure of sensitive electronic data. Establishing that the economic loss rule is not applicable to data breach claims may increase plaintiffs' likelihood of recovering monetary damages such as credit-monitoring costs.

It is nonetheless crucial to distinguish between the burden of proof plaintiffs must meet to recover damages at trial, from the lower burden of proving injury-in-fact to achieve standing.[233] Courts that improperly conflate injury (for standing purposes) and damages risk prematurely dismissing a claim on jurisdictional grounds that should have gone to trial.[234] The court in *Krottner* correctly observed that the jurisdictional standing requirements of federal courts are distinguishable from state-law issues related to tort damages.[235] This suggests that whether a plaintiff can recover damages for an increased risk of harm under state law is not germane to whether a plaintiff has standing to assert a claim for an increased risk of identity theft.[236] Courts that deny standing in data breach cases frequently rely too heavily on an estimation of plaintiffs' ability to

230. *Id.* at 122 n.59 (quoting Flagstaff Affordable Hous. Ltd. P'ship v. Design Alliance, Inc., 223 P.3d 664, 671 (Ariz. 2010)).

231. *See* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 300 (2005).

232. *Id.* at 300–01 (arguing that it is "simply unrealistic" to expect passive consumers to bargain with large companies due to an individuals' lack of commercial leverage).

233. Johnson, *supra* note 36, at 143–44 (highlighting the importance of this distinction because standing is a federal issue, whereas proof of damages implicates state tort law, meaning precedent established by federal courts should not serve as a guide to deciding what is essentially a state-law issue).

234. *See* Mark V. Tushnet, *The New Law of Standing: A Plea for Abandonment*, 62 CORNELL L. REV. 663, 663–64 (1977) (arguing that standing has become a surrogate for a full decision on the merits).

235. *See* Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) (dismissing the state-law claims).

236. *Id.*

recover damages, improperly employing the jurisdictional standing inquiry to address the merits of the plaintiffs' tort claims.[237] A plaintiff's relative likelihood of proving compensable damages, whether probable or improbable, should not bear on the determination of whether that plaintiff has standing to sue.[238]

CONCLUSION

Plaintiffs whose privacy and financial security are put at an elevated risk by the actions of another should not be turned away at the courthouse steps. When a person's sensitive digital data is compromised, the risk of future identity theft and the costs and emotional distress that ensue constitute an immediate harm worthy of justiciability. The *Reilly* court's analysis of Article III standing was flawed, and far too narrow, because it refused to acknowledge injury-in-fact for victims of data security breaches. The rule accepted by the *Pisciotta* and *Krottner* courts, which confers standing for plaintiffs in data breach cases, should control the analysis because the latent harm in defective medical device, toxic substance exposure, and environmental injury cases is analogous to the latent harm inherent in a heightened risk of future identity theft. These cases show that the risk of identity theft is not only a cognizable injury, but it is one that is remediable through injunctive relief in the form of credit-monitoring and identity theft security services. The circuit split created by the Third Circuit in *Reilly* should be resolved by adopting the decisions of the Seventh and Ninth Circuits to recognize injury-in-fact for plaintiff standing.

Permitting standing for increased risk of identity theft will bring this developing area of cybersecurity law in line with the Supreme Court's original intent of the standing doctrine, and it may help slow the escalating rate at which severe electronic security breaches occur by creating an incentive for corporations to meet the most rigorous security protocols possible to protect the privacy of their employees' and customers' personal information. Victims of data security breaches suffer a wide variety of immediate harms including the costs of protecting their identity, the hassle, emotional distress, and fear of being vulnerable to fraud, as well as the increased risk of future theft. These harms are very real and remediable, and when alleged by a plaintiff, should give courts little need to pause over a standing inquiry. And although data breach victims may fail to recover damages at trial, a jurisdictional standing inquiry should never serve as a

237. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 638 (7th Cir. 2007) (suggesting that a separate inquiry into a plaintiff's standing to bring a claim for increased risk of identity theft is necessary, even if the court later dismisses the case on the merits for inability to prove compensable damages for credit-monitoring costs).

238. *See supra* notes 155–58 and accompanying text.

court's opportunity to prematurely rule on the merits. Data security plaintiffs, whether they ultimately are awarded relief or not, deserve their day in court.