

2013

Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits

Patricia Cave

Follow this and additional works at: <https://scholarship.law.edu/lawreview>



Part of the [Administrative Law Commons](#), [Constitutional Law Commons](#), [Consumer Protection Law Commons](#), [Courts Commons](#), and the [Legislation Commons](#)

Recommended Citation

Patricia Cave, *Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 Cath. U. L. Rev. 765 (2013).

Available at: <https://scholarship.law.edu/lawreview/vol62/iss3/5>

This Comments is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Law Review by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.

Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits

Cover Page Footnote

J.D. and Institute for Communications Law Studies Certificate Candidate, May 2014, Catholic University of America, Columbus School of Law; B.S., 2011, Virginia Polytechnic Institute and State University. The author wishes to thank her mother for providing the inspiration to always work toward her goals; her siblings for their unending friendship; and her friends for their unwavering support.

GIVING CONSUMERS A LEG TO STAND ON: FINDING PLAINTIFFS A LEGISLATIVE SOLUTION TO THE BARRIER FROM FEDERAL COURTS IN DATA SECURITY BREACH SUITS

Patricia Cave⁺

For hackers, “[t]he holy grail . . . is the account information.”¹ In recent years, the prevalence of data security breaches has increased, culminating in one of the largest breaches in history, which impacted over seventy-seven million users.² The proliferation of smart-phones and tablet devices has promoted a virtual marketplace that has contributed to the reality where consumers conduct many aspects of their lives solely through the internet.³ In a world in which consumers perform countless online transactions, ranging from banking to purchasing holiday gifts through online retailers such as Amazon.com, data breaches raise questions about the security of names, social security numbers, addresses, and other personal information collected by companies.⁴ Each year security breaches and security-breach notification laws cost businesses billions of dollars.⁵ Security breaches also undermine consumer confidence, resulting in further harm to the economy.⁶

In 2011, identity theft ranked as the most frequent consumer complaint submitted to the Federal Trade Commission (FTC) for the twelfth year in a

⁺ J.D. and Institute for Communications Law Studies Certificate Candidate, May 2014, Catholic University of America, Columbus School of Law; B.S., 2011, Virginia Polytechnic Institute and State University. The author wishes to thank her mother for providing the inspiration to always work toward her goals; her siblings for their unending friendship; and her friends for their unwavering support.

1. Jessica Silver-Greenberg & Nelson D. Schwartz, *MasterCard and Visa Investigate Data Breach*, N.Y. TIMES, Mar. 30, 2012, at B1.

2. Liana B. Baker & Jim Finkle, *Sony Playstation Suffers Massive Data Breach*, REUTERS, Apr. 26, 2011, available at <http://www.reuters.com/assets/print?aid=USTRE73P6WB20110426>; Nick Bilton & Brian Stelter, *Sony Says PlayStation Hacker Got Personal Data*, N.Y. TIMES, Apr. 27, 2011, at B1.

3. See, e.g., *Smartphones: Changing the Way Businesspeople Work and Live*, RINGCENTRAL (Apr. 10, 2012), <http://blog.ringcentral.com/2010/04/smartphones-changing-the-way-business-professionals-work-and-live.html> (noting the increasing role such devices are playing in the personal and professional lives of many).

4. See Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1154–55 (1997) (discussing the increased use of computers and the internet and the resulting concerns about loss of personal information and privacy).

5. Eduardo M. Gonzalez, Comment, *The New Arizona Data Security Breach Law: A Step in the Right Direction, But Unlikely to Prevent Identity Theft or Compensate Consumers*, 40 ARIZ. ST. L.J. 1349, 1355 (2008) (noting an estimated cost of \$48 billion per year to the retail sector alone).

6. *Id.*

row.⁷ Identity thieves use personal information in a variety of ways, including opening a new line of credit in the victim's name, opening fraudulent banking accounts, making purchases using the victim's existing credit card or bank account, improperly using social security numbers to apply for jobs, and securing cable, satellite, or wireless cell phone services.⁸ Identity theft arising out of data security breaches amounted to 1.7% of claims filed with the FTC in 2011.⁹ Although the percentage appears low, the FTC's inclusion of the category is itself significant. Previously, identity theft due to data breaches was not separately identified; thus the FTC's recognition demonstrates a growing trend of recognizing the issue.¹⁰

In addition to the rarely read terms-of-use agreements and the lack of consumer awareness of exactly how much personal information is aggregated, shared, and stored by companies, consumers face numerous barriers to bringing a successful claim against a company that exposes their information.¹¹ The FTC, an independent regulatory agency charged with preventing unfair or deceptive practices affecting consumers, establishes rules and regulations and

7. FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JANUARY – DECEMBER 2011, at 3 (2012), available at <http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf> (finding that fifteen percent of complaints involved identity thefts).

8. IDENTITY THEFT RES. CTR., IDENTITY THEFT: THE AFTERMATH 2007, at 1, 7–8, available at http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf. Identity theft victims face many actual and psychological challenges including the inability to clear negative credit records, an increase in insurance and credit card rates, criminal arrest warrants improperly issued for the innocent victim resulting from financial or other crimes committed by the identity thief, and severe negative emotional impacts. See Press Release, Identity Theft Resource Center, ITRC's 5th Annual Aftermath Study Released: An Analysis of Identity Theft Through the Victim's Eyes (June 3, 2008), available at http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2007.shtm l.

9. See FED. TRADE COMM'N, *supra* note 7, at 12.

10. See *id.*

11. See Derek A. Bishop, Note, *No Harm No Foul: Limits on Damages Awards for Individuals Subject to a Data Breach*, 4 SHIDLER J.L. COM. & TECH. 12, 23 (2008) (discussing the challenges plaintiffs face in bringing data breach suits based on negligent database management); see also Kenneth K. Dort, *Recent Trends in Cyberspace Law: Data Security and Privacy*, in UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 139 (2012), available at 2012 WL 2244546, at *9 (stating that “courts have generally not provided relief . . . unless the plaintiff is able to demonstrate a cognizable harm,” such as financial damage); Timothy H. Madden, *Data Breach Class Action Litigation – A Tough Road for Plaintiffs*, 55 BOS. B.J. 27, 27–28 (2011) (acknowledging that “courts have been reluctant to allow [data breach] litigation to proceed past the earliest stages”); Amanda Blades, Note, *Can't Get No Satisfaction: The Consequences of Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007) for Potential Victims of Identity Theft, 33 S. ILL. U. L.J. 509, 511 (2009) (noting that “courts have refused to recognize the compromising of personal information as a cognizable injury without the actual fraudulent use of the that information”).

seeks monetary redress and relief for conduct that is injurious to consumers.¹² The FTC has not yet adopted data privacy regulations addressing liability in data security breach situations.¹³

Congress has neither provided the FTC with authority to promulgate data security regulations, nor has it passed any comprehensive data privacy legislation imposing standards on all private entities, although many bills have been proposed in recent years.¹⁴ However, Congress has passed a range of laws imposing privacy requirements on public and private entities that manage, aggregate, and share consumer information.¹⁵ Meanwhile, states have addressed the issue individually, passing data privacy legislation on a piecemeal basis.¹⁶ These efforts primarily focus on notification statutes requiring companies to follow certain procedures after discovering a data breach.¹⁷ The combination of a lack of uniform statutory guidance about

12. See *About the Federal Trade Commission*, FED. TRADE COMM'N, <http://www.ftc.gov/ftc/about.shtm> (last visited Mar. 15, 2013).

13. See Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 65 ADMIN. L. REV. 127, 170 (2008) (stating that “[n]o guidelines exist under which the Commission will act or refrain from acting if a data security breach occurs”).

14. See, e.g., Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011) (providing notice and procedural requirements for entities that maintain databases of personal information, permitting federal and state authorities to impose civil penalties for violations, and creating causes of action for violations of the statute); Data Breach Notification Act of 2011, S. 1408, 112th Cong. (2011) (requiring disclosure of security breaches); Cyber-Security Enhancement and Consumer Data Protection Act of 2006, H.R. 5318, 109th Cong. (2006) (imposing a \$50,000 fine for each day an individual fails to provide notice of a major security breach, up to one million dollars); Data Accountability and Trust Act (DATA), H.R. 4127, 109th Cong. (2005) (requiring covered entities to establish various security policies, such as identifying an individual responsible for overseeing data security); Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005) (amending the Fair Credit Reporting Act to require improved protections for financial data); Personal Data Privacy Security Act of 2005, S. 1789, 109th Cong. (2005) (requiring commercial entities to implement a comprehensive data privacy and security program for protecting sensitive personally identifiable information and notifying all U.S. residents whose personal information has been accessed); Identity Theft Protection Act, S. 1408, 109th Cong. (2005) (requiring covered entities to develop and implement a program for security of sensitive personal information including administrative, technical, and physical safeguards); Notification of Risk to Personal Data Act, S. 1326, 109th Cong. (2005) (requiring minimum data security and notification procedures).

15. See, e.g., Privacy Act, 5 U.S.C. § 552a (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 680–6809 (2006); CAN-SPAM Act of 2003, 15 U.S.C. § 7701 (2006); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2006 & Supp. 2011).

16. See Vincent Serpico, Denise Landers & Damon A. Terrill, *Making Sense of U.S. State Data Privacy Laws*, 119 BANKING L.J. 462, 463 (2002).

17. See, e.g., ALASKA STAT. § 45.48.010 (2012) (requiring notification of breach); ARIZ. REV. STAT. ANN. § 44-7501 (Supp. 2012) (requiring notification and enforcement by the attorney general); ARK. CODE ANN. §§ 4-110-101 to -108 (2011) (requiring individuals and businesses to

database management obligations and limited remedies available to consumers, results in varied court decisions as to whether a consumer whose account information has been exposed to an unauthorized third-party, but has not yet been used fraudulently, has standing to bring a claim.¹⁸

Some courts consider the mere increased risk of identity theft as too hypothetical or conjectural to satisfy the constitutional standing requirement

protect sensitive personal information and promptly disclose security breaches); COLO. REV. STAT. § 6-1-716 (2012) (requiring notification of breach); CONN. GEN. STAT. ANN. § 36a-701b (West 2011) (requiring notification of breach and stating that noncompliance constitutes an unfair trade practice punishable by the attorney general); DEL. CODE ANN. tit. 6, § 101-104 (2005 & Supp. 2012) (requiring notification of breach and enforcement by the attorney general); FLA. STAT. § 817.5681 (2006) (requiring notification of breach without unreasonable delay and establishing civil penalties for non-compliance up to \$500,000); GA. CODE ANN. §§ 10-1-912 (2009) (requiring notification of breach to consumers and, in the case of a breach affecting more than ten thousand residents, requiring notification to consumer reporting agencies); IOWA CODE ANN. § 715C.2 (West Supp. 2012) (requiring notification of breach and giving the attorney general authority to recoup damages on behalf of injured parties); LA. REV. STAT. ANN. §§ 51:3071-77 (2012) (requiring notification of breach); ME. REV. STAT. ANN. tit. 10, § 1348 (West 2009 & Supp. 2012) (requiring notification of breach); MASS. GEN. LAWS ANN. ch. 93H, §§ 2-6 (West Supp. 2012) (imposing regulations to safeguard state residents' personal information and requiring notification of breach requirements subject to attorney general action in case of violations); MICH. COMP. LAWS § 445.72 (2011) (requiring notification of breach and imposing a civil fine or imprisonment for violations); N.J. STAT. ANN. § 56:8-163 (West 2012) (requiring notification of breach to residents and consumer reporting agencies when a thousand or more people are affected by a security breach); N.C. GEN. STAT. § 75-65 (2011) (requiring notification of breach and prohibiting a private cause of action unless that individual is in fact injured because the violation); 73 PA. CONS. STAT. § 2303 (2011) (requiring notification of breach to consumers and reporting agencies without unreasonable delay and granting the attorney general exclusive authority to bring an action for violation of the Unfair Trade Practices and Consumer Protection Law); S.C. CODE ANN. § 39-1-90 (Supp. 2012) (requiring notification of breach and providing injured South Carolinian the opportunity to bring an action to seek actual damages, an injunction to enforce compliance, and to recover attorney's fees); VT. STAT. ANN. tit. 9, § 2435 (2006 & Supp. 2012) (requiring notification of data security breach and giving the attorney general and the state's attorney exclusive authority to enforce the requirements); WIS. STAT. § 134.98 (2009) (requiring notice in cases of security breach); D.C. CODE § 28-3852 (2011) (requiring notification of breach to a resident whose personal information was compromised and permitting injured residents to collect actual damages, not including pain and suffering). A few states have already enacted comprehensive data protection statutes concerning the personal information of their residents. *See, e.g.*, CAL. CIV. CODE § 1798.81 (West 2009) (imposing a duty on businesses to take reasonable care in handling consumers' personal identification information).

18. *See Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that the plaintiff had standing after a laptop containing unencrypted personal information was stolen); *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (finding standing on the basis of increased risk of future harm). *But see Katz v. Pershing, L.L.C.*, 672 F.3d 64, 80 (1st Cir. 2012) (holding that a plaintiff could not satisfy Article III's standing requirement because she did not allege actual or impending injury); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) (holding that alleged risk of future harm is insufficient to establish standing), *cert. denied*, 132 S. Ct. 2395 (2012).

that plaintiffs suffer concrete injury-in-fact.¹⁹ Other courts, however, show a willingness to consider standing as a low threshold requirement.²⁰ Courts willing to acknowledge the increased threat of identity theft have analogized the facts to cases involving defective medical devices, toxic substance exposure, and environmental injury.²¹ However, plaintiffs must also allege actual, compensable damages in claims under common law theories of negligence, emotional distress, or breach of contract.²² These suits are likely to be, and have been, dismissed for failure to state a claim on the premise that the plaintiff's injury is not compensable under state law despite conquering the initial standing hurdle.²³

This Comment discusses potential solutions that would allow plaintiffs to successfully bring claims centered on data security breaches in federal court. The Comment begins by considering standing as a requirement imposed by Article III of the Constitution and reviews the inconsistencies of data breach standing jurisprudence in the various courts of appeals. Next, it discusses the courts' rationales for granting or denying standing and analyzes plaintiffs' subsequent hurdle of proving compensable injury for claims based on common law theories of negligence and breach of contract. Next, this Comment considers the inadequacy of already-enacted federal and state legislation in the area of data privacy. Finally, this Comment concludes that the most appropriate solution to the issue presented is for Congress to debate and adopt comprehensive data privacy legislation. Any legislation should provide both governmental enforcement and a private cause of action for consumers whose information has been exposed to an unauthorized third-party.

19. See *Katz*, 672 F.3d at 80; *Reilly*, 664 F.3d at 43; *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307 (S.D.N.Y. June 25, 2010) (concluding that plaintiffs' "future-oriented, hypothetical, and conjectural" claims were insufficient to establish standing); *Allison v. Aetna, Inc.*, Civ. A. No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010) (holding that an allegedly heightened risk of identity theft is too speculative to confer standing); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1050 (E.D. Mo. 2009) (emphasizing the need for immediate threat of harm to confer standing).

20. *Pisciotta*, 499 F.3d at 634.

21. See *id.* at 634 n.3; see also *Blades*, *supra* note 11, at 513–18 (examining the comparison between medical monitoring and identity theft protection).

22. See *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162 (1st Cir. 2011) (stating that under Maine negligence law, damages must be reasonably foreseeable); *Pisciotta*, 499 F.3d at 639 (noting that actual injury is required to recover in the absence of statutory law); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009) (noting that state law required the claim to be dismissed for failure to allege appreciable harm), *aff'd*, 380 F. App'x. 689 (9th Cir. 2010); *Bishop*, *supra* note 11, at 23 (discussing plaintiffs' difficulty in alleging actual compensable damages in data breach suits).

23. *Pisciotta*, 499 F.3d at 639 (stating that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy"); *Ruiz*, 622 F. Supp. 2d at 913 (dismissing a job applicant's claim against a prospective employer because California negligence law required more than an increased risk of future identity theft to allege a compensable injury).

I. CONSTITUTIONAL UNDERPINNINGS OF STANDING PROVIDE A BACKDROP FOR DATA SECURITY

A. *Standing Limits the Power of the Judiciary in Order to Respect Separation of Powers and Judicial Efficiency*

Article III of the U.S. Constitution articulates the power of the federal judiciary.²⁴ Federal courts are courts of limited jurisdiction and may only hear actual, live “cases and controversies.”²⁵ In addition to the other justiciability doctrines of mootness,²⁶ ripeness,²⁷ and political question,²⁸ standing ensures that the proper plaintiff brings a matter to court for adjudication.²⁹

Standing is “built on a single basic idea—the idea of separation of powers.”³⁰ Justice Antonin Scalia once wrote that “the law of standing roughly restricts courts to their traditional undemocratic role of protecting individuals and minorities against . . . the majority, and excludes them from . . . prescribing how the other two branches should function in order to serve the interest of the majority itself.”³¹ The standing doctrine assists in determining the role of the judiciary.³² Courts have declined to expand their

24. U.S. CONST. art. III.

25. *Id.* § 2.

26. The mootness doctrine requires that an actual controversy exist during the entire judicial review rather, and not only, at the time the suit is filed. *See Note, The Mootness Doctrine in the Supreme Court*, 88 HARV. L. REV. 373, 375 (1974). *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES (4th ed. 2011).

27. The ripeness doctrine attempts to avoid premature adjudication of disputes by reviewing “the fitness of the issues for judicial decision” and the “hardship to the parties of withholding court consideration.” Gene R. Nichol, Jr., *Ripeness and the Constitution*, 54 U. CHI. L. REV. 153, 161 (1987) (quoting *Abbott Labs. v. Gardner*, 387 U.S. 136, 148 (1967)); *see also* CHEMERINSKY, *supra* note 26, at 104–14.

28. The political question doctrine requires a determination on whether a matter has been committed by the Constitution to the political branches of government. *See Baker v. Carr*, 369 U.S. 186, 210 (1962); *see also* CHEMERINSKY, *supra* note 26, at 130–51.

29. CHEMERINSKY, *supra* note 26, at 59.

30. *Allen v. Wright*, 468 U.S. 737, 752 (1984); *see also* *Lewis v. Casey*, 518 U.S. 343, 353 n.3 (1996) (acknowledging a “separation-of-powers component” to the standing doctrine and that actual injury is a requirement to prevent frivolous claims from being pursued in the judicial system).

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

32. *See* CHEMERINSKY, *supra* note 26, at 60; *see also* Heather Elliott, *Congress’s Inability to Solve Standing Problems*, 91 B.U. L. REV. 159, 169–70 (2011) (stating that standing prevents courts from hearing cases better left to the political branches and that standing can be used effectively to prevent improper efforts to control the Executive Branch); William Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 222 (1988) (stating that the purposes of the doctrine of standing include “preventing the anti-majoritarian federal judiciary from usurping the policy-making functions of the popularly elected branches”); Robert J. Pushaw, Jr., *Article III’s Case/Controversy Distinction and the Dual Functions of Federal Courts*, 69 NOTRE DAME L.

own jurisdiction beyond live cases and controversies to avoid issuing advisory opinions and to prevent exceeding the judicial branch's political capacity by encroaching on the powers of the other branches of government.³³

The architects of the federal judiciary created the standing requirement to increase judicial efficiency by ensuring that the plaintiff bringing a suit is personally invested in or affected by the adjudication.³⁴ Justice William Brennan emphasized in *Baker v. Carr* that a plaintiff must allege "such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination of difficult constitutional questions."³⁵ While courts do not consider the merits of a claim at the early stage of analysis associated with a justiciability determination,³⁶ "[t]he essence of a true standing question is . . . [whether] the plaintiff ha[s] a legal right to judicial enforcement of an asserted legal duty," a question that can be and has been interpreted as requiring an evaluation of the merits.³⁷ Courts should dismiss the suit "[i]f the party bringing the litigation is not the appropriate party."³⁸ Some critics of the Court's standing jurisprudence consider the use of standing as a way to avoid controversial cases by disposing of a claim in the name of judicial efficiency and separation of powers.³⁹

REV. 447, 519–20 (1994) (arguing that a restrictive standing doctrine with a high constitutional bar plays an important, and even essential, role in managing judicial functions under Article III.).

33. CHEMERINSKY, *supra* note 26, at 60; Pushaw, *supra* note 32, at 512.

34. CHEMERINSKY, *supra* note 26, at 59–60.

35. *Baker v. Carr*, 369 U.S. 186, 204 (1962).

36. *Id.* at 196–98.

37. Fletcher, *supra* note 32, at 229.

38. LEE EPSTEIN & THOMAS G. WALKER, CONSTITUTIONAL LAW FOR A CHANGING AMERICA: INSTITUTIONAL POWERS AND CONSTRAINTS 115–16 (6th ed. 2007).

39. See LISA A. KLOPPENBERG, PLAYING IT SAFE: HOW THE SUPREME COURT SIDESTEPS HARD CASES AND STUNTS THE DEVELOPMENT OF THE LAW 1 (2001) (arguing that the Supreme Court uses standing as a way to dispense of "socially sensitive" cases, particularly race-centered cases); Gene R. Nichol, Jr., *Abusing Standing: A Comment on Allen v. Wright*, 133 U. PA. L. REV. 635, 639–42 (1985) (criticizing the Burger Court for calling for the dismissal of cases without meaningful examination of the plaintiff's interests, particularly in cases brought by minorities by adjusting the requirements of the standing analysis); Mark V. Tushnet, *The New Law of Standing: A Plea for Abandonment*, 62 CORNELL L. REV. 663 (1977); see also *City of L.A. v. Lyons*, 461 U.S. 95, 112–13 (1983) (holding that an African-American man, who had been nearly knocked unconscious as a result of a choke-hold administered by a Los Angeles Police Department officer, lacked standing to sue for injunctive relief because he could not show that it would occur again); Mark Starr & Janet Huck, *The Chokehold Controversy*, NEWSWEEK, May 24, 1982, at 32 (examining the race component in the *Lyons* decision). See generally Daniel E. Ho & Erica L. Ross, *Did Liberal Justices Invent the Standing Doctrine? An Empirical Study of the Evolution of Standing, 1921–2006*, 62 STAN. L. REV. 591, 610–11 (2010) (analyzing decisions throughout history using data processing and concluding that standing is used to insulate administrative agencies from judicial review).

1. Understanding Constitutional Standing

Article III, Section 2 of the U.S. Constitution restricts federal court jurisdiction to specific “cases” or “controversies.”⁴⁰ With little guidance from the text of the Constitution, the Supreme Court has determined that standing to bring a claim requires three essential elements.⁴¹ First, the plaintiff must have “suffered an ‘injury in fact’ – an invasion of a legally protected interest.”⁴² The injury complained of must be “actual or imminent, not ‘conjectural’ or ‘hypothetical.’”⁴³ Second, a plaintiff’s claim must arise from an injury that “fairly can be traced to the challenged action of a defendant.”⁴⁴ Third, a favorable court decision must be able to redress the plaintiff’s injury.⁴⁵ The plaintiff bears the burden to establish all three elements.⁴⁶ The issue of standing, a question of subject matter jurisdiction, can be raised by the parties or sua sponte by the court at any point during the litigation.⁴⁷ For an injury to sufficiently confer standing in a civil suit, the plaintiff must personally suffer the injury in question.⁴⁸ It is “clear that injuries to common law, constitutional, and statutory rights are sufficient” to confer standing on a plaintiff.⁴⁹

2. Differentiating Statutory Standing

In addition to the common law and constitutionally based causes of action, “Congress may create a statutory right or entitlement, . . . which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury [without the] statute.”⁵⁰ Often, Congress integrates a private right of action against a violator of a statute within the statute’s language.⁵¹

40. U.S. CONST. art. III, § 2.

41. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

42. *Id.*

43. *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (quoting *Lyons*, 461 U.S. at 102).

44. *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976).

45. *Lujan*, 504 U.S. at 561 (quoting *Simon*, 426 U.S. at 38).

46. *Id.*

47. *CHEMERINSKY*, *supra* note 26, at 62. See, e.g., *Pisciotta v. Old Nat’l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007).

48. *Lujan*, 504 U.S. at 565–68 (denying standing because the plaintiffs could not show that the failure to preserve endangered species abroad would cause the plaintiffs personal harm); see also *Lyons*, 461 U.S. at 109–10 (holding that a man lacked a personalized injury for which to seek an injunction against the Los Angeles Police Department’s use of the chokehold because it was uncertain that this particular plaintiff would be injured in the future by another chokehold).

49. *CHEMERINSKY*, *supra* note 26, at 69.

50. *Warth v. Seldin*, 422 U.S. 490, 514 (1975); see also *Tushnet*, *supra* note 39, at 153 (stating that “legislators could create new interests, the violation of which would give rise to standing.”).

51. See, e.g., *Fed. Election Comm’n v. Akins*, 524 U.S. 11, 19 (1998) (holding that Congress had the authority to create the right to information about political committees, a violation of which was sufficient to confer standing on any person); *Trafficante v. Metro. Life Ins. Co.*, 409 U.S. 205, 209, 211 (1972) (recognizing that a white woman had standing because an apartment complex owner’s discrimination against black applicants deprived her of a right to be

The Court in *Lujan v. Defenders of Wildlife*, however, struck down a provision of the Endangered Species Act permitting anyone to file suit against a violator of the Act as an unconstitutional attempt by Congress to “transfer [power to execute the law] from the President to the courts,” and a violation of Article III’s case or controversy requirement.⁵² In contrast to *Lujan* in which the statute did not require the plaintiff to have been “affected” by a statutory violation, when the legislature provides clear evidence of its intent to grant persons affected by violations of a statute the right to sue, the act of Congress comports with Article III standing principles.⁵³ When a court considers whether statutory standing exists, it considers whether the particular plaintiff can properly avail herself of the private right of action created by the statute.⁵⁴ Statutory standing essentially provides a route to federal court by “elevat[ing] injuries that were not previously legally cognizable to the status of legally enforceable rights.”⁵⁵

Various types of injuries satisfy standing.⁵⁶ The Court acknowledged that aesthetic harm can be sufficient to confer standing.⁵⁷ While willing to recognize standing in some cases of economic or aesthetic harm, the Court is unwilling to recognize standing for other proposed injuries, such as marital happiness.⁵⁸ With a lack of guiding principles in standing jurisprudence, the application of the doctrine has often depended on the type of injury suffered. This confusion has led to the current split in federal courts on whether plaintiffs in data security breach suits have suffered an injury sufficient to confer Article III standing.⁵⁹

free from the adverse consequences of racial discrimination created by the Civil Rights Act of 1968).

52. *Lujan*, 504 U.S. at 579.

53. See *Gwaltney of Smithfield, Ltd. v. Chesapeake Bay Found.*, 484 U.S. 49, 70–71 (1987) (Scalia, J., concurring in part and concurring in the judgment) (finding that the Clean Water Act’s citizen suit provision embodies the constitutional requirement of injury in the preliminary determination of standing). The Clean Water Act provides that “any citizen” may bring suit for violations of the Act. 33 U.S.C. § 1365(g) (2006). The Act defines “citizen” as “a person or persons having an interest which is or may be adversely affected.” *Id.*

54. Radha A. Pathak, *Statutory Standing and the Tyranny of Labels*, 62 OKLA. L. REV. 89, 91 (2009).

55. John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1228 (1993).

56. See, e.g., *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 686–89 (1973) (holding that a claim of an aesthetic or environmental harm is sufficient to constitute an injury for Article III standing purposes).

57. See *Lujan*, 504 U.S. at 562–63.

58. See, e.g., *Allen v. Wright*, 468 U.S. 737, 755–56 (1984) (denying stigmatization caused by the government’s discriminatory taxation policy of providing tax exemptions to private schools that used racially discriminatory practices as a sufficient injury for standing); *Roe v. Wade*, 410 U.S. 113, 128 (1973) (refusing to acknowledge possible future harm to marital happiness as sufficient to confer Article III standing).

59. Compare *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (denying standing to a plaintiff whose personal information was inadvertently disclosed), and *Reilly v. Ceridian Corp.*,

B. Courts Disagree on Whether Data Breach Suit Plaintiffs Have Suffered Actual or Imminent Harm

When the personal information exposed in a data breach has not yet been used fraudulently, plaintiffs face an uphill battle in demonstrating an injury sufficient for Article III standing.⁶⁰ While courts generally have refused to recognize the increased threat of identity theft as a cognizable injury for standing purposes, a few have recognized that, in certain circumstances, the lack of fraudulent use is not an absolute bar to a claim.⁶¹

1. Increased Threat of Future Harm Caused by the Data Breach Is Sufficient to Confer Article III Standing in Some Courts

The Seventh and Ninth Circuit Courts of Appeals have found Article III standing when proof exists that an unauthorized third-party accessed the plaintiff's personal information, even if the personal information has not yet been used fraudulently.⁶² In reaching their conclusions, these courts have endorsed the view that alleging future harm can be sufficient for standing if there is "danger of sustaining some *direct* injury as the result of the challenged . . . conduct and the injury or threat of injury is both real and immediate, not conjectural or hypothetical."⁶³ To determine whether a consumer faces a risk of future harm in the form of identity theft after a data breach exposes their

664 F.3d 38, 43 (3d Cir. 2011) (finding potential harm from data breaches too conjectural to confer standing), *cert. denied*, 132 S. Ct. 2395 (2012), with *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (finding that the data breaches presented a "credible threat of real and immediate harm"), and *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (recognizing an increased risk of future harm as sufficient for standing).

60. *Dort*, *supra* note 11, at *10 (arguing that the Information Revolution presents a challenge that must be resolved to permit businesses to grow while protecting consumers); *Madden*, *supra* note 11, at 27–28; Jacob W. Schneider, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 288 (2009) (stating that an uphill battle results for consumers who are unable to show damages); *Bishop*, *supra* note 11, at 23 (acknowledging that the "courts have required that the [personal] information be used fraudulently"); *Blades*, *supra* note 11, at 511 (discussing the standing hurdle faced by plaintiffs in data breach suits and how *Pisciotta* should be overturned on policy considerations).

61. *Krottner*, 628 F.3d at 1143; *Pisciotta*, 499 F.3d at 634; *see also* Gary Zhao, *Claridge v. RockYou, Inc.: "Value" Inherent in Consumers' Personally Identifiable Information*, 2011-SEP BUS. L. TODAY 1, 1 (2011) (commenting about the tendency for courts to dismiss consumer suits for failure to meet the injury-in-fact requirement of standing, among other hurdles).

62. *Krottner*, 628 F.3d at 1143 (finding that the plaintiff adequately alleged Article III standing by alleging future harm as a result of the data breach); *Pisciotta*, 499 F.3d at 634 ("[T]he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions").

63. *Scott v. Pasadena Unified Sch. Dist.*, 306 F.3d 646, 656 (9th Cir. 2002) (quoting *City of L.A. v. Lyons*, 461 U.S. 95, 102 (1983)).

personal information, these courts have relied on the reasoning in defective medical device, toxic substance exposure, and environmental injury cases.⁶⁴

In *Pisciotta v. Old National Bancorp*, the Seventh Circuit recognized that in circumstances where an unauthorized third-party accesses the information through a “sophisticated, intentional and malicious” manner, a perceived increased risk of identity theft sufficiently establishes standing.⁶⁵ In *Pisciotta*, the hosting facility of a marketing website used for completing online applications for banking services suffered a security breach.⁶⁶ Plaintiffs brought a class action suit against the marketing website and hosting service alleging negligence and breach of contract claims.⁶⁷ After considering the rationales of its sister courts in dismissing cases with similar facts, the Seventh Circuit was satisfied that “a threat of future harm or . . . an act which harms the plaintiff only by increasing the risk of future harm” is sufficient to confer standing when the increase in risk was caused by the defendant’s actions.⁶⁸ Once a plaintiff’s level of injury reaches the increased risk of harm threshold, standing has been met.⁶⁹

Similarly, in *Krottner v. Starbucks Corp.*, the Ninth Circuit held that the theft of a laptop computer from a Starbucks containing unencrypted personal data of Starbucks employees was a “credible threat of real and immediate harm.”⁷⁰ The court hypothesized that its conclusion might be different

64. As data security breach suits are a relatively new phenomenon, it is helpful to apply the rationale from these similar fields in deciding standing issues. See *Pisciotta*, 499 F.3d at 632, 634. The similarity of medical devices, toxic substances, environmental injury, and data breach cases arises from a plaintiff’s increased risk of harm resulting from a defendant’s action. Some courts, however, have refrained from expanding the scope of what constitutes an injury for purposes of standing because toxic tort and defective medical device cases “‘directly involve human health and safety,’ while ‘credit monitoring cases . . . do not.’” See Chad Pinson, *New Legal Frontier: Mass Information Loss and Security Breach*, 11 SMU SCI. & TECH. L. REV. 27, 47 (2007) (quoting *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185PHVSRB, 2005 WL 2465906, at *4 (D. Ariz. 2005)).

65. *Pisciotta*, 499 F.3d at 632, 634.

66. *Id.* at 631–32.

67. *Id.* at 632.

68. *Id.* at 634.

69. *Id.* Interestingly, in *Lambert v. Hartman*, in which the plaintiff filed a claim based on the publication of personal information as a result of the state’s publication of a traffic citation, the Sixth Circuit Court of Appeals considered purchasing credit monitoring service notification as sufficient damage in considering Article III standing. 517 F.3d 433, 438 (6th Cir. 2008); see also *Holmes v. Countrywide Fin. Corp.*, No. 5:08-CV-00205 R, 2012 WL 2873892, at *4 (W.D. Ky. July 12, 2012) (relying on *Lambert* to find the purchase of credit monitoring services and change of telephone services as sufficient to “satisfy Article III’s requirement of an ‘actual or imminent injury’”).

70. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010); see also *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848, at *5 (N.D. Cal. Nov. 11, 2011) (stating that “where sensitive personal data, such as names, addresses, social security numbers and credit card numbers, is improperly disclosed or disseminated into the public, increasing the risk of future harm, injury-in-fact has been recognized”). Cf. *Randolph v. ING Life Ins.*

“if . . . the Plaintiffs had sued based on the risk that [the laptop] would be stolen at some point in the future.”⁷¹ The *Krottner* court looked to *Pisciotta* and its comparison to toxic substance, medical monitoring, and environmental claims to support its own finding.⁷²

2. Courts Disagree on Standing in Security Breach Suits Without Proof of Unauthorized Third Party Access or Proof of Actual Economic Harm

In contrast to the Seventh and Ninth Circuits, the First and Third Circuits have held that the increased risk of identity theft is an insufficient injury to meet the requirements of Article III standing.⁷³ These courts rationalize their holdings based on the speculative nature of any increased risk of future harm⁷⁴—until the chain of “conjectures come[s] true, [plaintiffs] have not suffered any injury; there has been no misuse of the information, and thus, no harm.”

In *Katz v. Pershing*, the First Circuit emphasized that relying on too many conjectures “would stretch the injury requirement past its breaking point.”⁷⁵ The plaintiff in *Katz* maintained a brokerage account with a firm that she felt failed to adequately secure her information.⁷⁶ The court was convinced that

& Annuity Co., 486 F. Supp. 2d 1, 6–8 (D.D.C. 2007) (refusing to find standing when a computer containing the plaintiff’s personal information was stolen during a burglary caused an increased risk of identity theft); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 689, 690 (S.D. Ohio 2006) (dismissing a class action suit for lack of standing where an unauthorized third-party accessed personal information of 96,000 customers).

71. *Krottner*, 628 F.3d at 1143. For the *Krottner* court, in addition to finding an increased risk of identity theft as sufficient to confer standing, generalized anxiety caused by the theft of the laptop was a sufficiently concrete injury. *Id.* at 1142.

72. *Id.*

73. *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012) (holding that, because a plaintiff cannot “identify any incident in which her data has ever been accessed by an unauthorized person, she cannot satisfy Article III’s requirement of actual or impending injury”); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) (holding that the plaintiff’s “alleged risk of future injury is nothing more than speculation” and cannot be considered actual or impending), *cert. denied*, 132 S. Ct. 2395 (2012); *see also* *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) (concluding that “[p]laintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural”); *Allison v. Aetna, Inc.*, Civil Action No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. March 9, 2010) (holding that “it is highly speculative that [hackers] obtained any other information that would be necessary to commit identity theft” after plaintiff alleged that hackers only obtained his email address); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1050 (E.D. Mo. 2009) (stating that a “[p]laintiff must allege that he has sustained or is in immediate danger of sustaining some direct injury as a result of the challenged conduct”).

74. *Reilly*, 664 F.3d at 42 (stating that the speculations include assuming that the hacker: “(1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [the plaintiff] by making unauthorized transactions in [the plaintiff’s] name”).

75. *Katz*, 672 F.3d at 80.

76. *Id.* at 70. Among her allegations, the plaintiff maintained that (1) her information was accessible in unencrypted form by authorized users around the clock and could be accessible to

without any allegation of actual improper access the plaintiff lacked standing to assert her claims.⁷⁷

In *Reilly v. Ceridian Corp.*, the Third Circuit agreed, noting that absent any identifiable proof that the plaintiff's information had been accessed or used, mere knowledge of infiltration of a database firewall was too conjectural.⁷⁸ According to the Third Circuit, until the chain of "conjectures come[s] true, [plaintiffs] have not suffered any injury; there has been no misuse of the information, and thus, no harm."⁷⁹

The First and Third Circuits' holdings are distinguishable from *Pisciotta's* sophisticated and malicious intrusion claim⁸⁰ or *Krottner's* stolen unencrypted data claim.⁸¹ These opinions demonstrate a hesitance to follow the recent trend that recognizes increased likelihood of harm as sufficient to confer standing because "the requirement of standing is firmly rooted in the Constitution and is not subject to whim."⁸² Typically judges and commentators warn against setting precedent on jurisdictional issues based on public policy motives.⁸³ This underlying principle of limiting courts' jurisdiction aligns with the purpose of the justiciability doctrine to prevent the judiciary from unconstitutionally usurping powers best left to the political branches.⁸⁴

3. Plaintiffs Fail to Demonstrate Injury to Recover Damages in Negligence and Contract-Based Claims Despite a Court's Finding of Standing

Even in jurisdictions that accept increased risk of future identity theft as sufficient to confer Article III standing, plaintiffs still struggle with

hackers; (2) unauthorized access to her information was improperly monitored; and (3) procedures for end-user authentication were inadequate to protect her information. *Id.*

77. *Id.* at 79.

78. *Reilly*, 664 F.3d at 44.

79. *Id.* at 42; see also Stephen F. Ambrose, Jr., Joseph W. Felb & Walter F. Zalenski, *Survey of Significant Consumer Privacy Litigation in the United States in 2006*, 62 BUS. LAW. 651, 651 (2007) (commenting that plaintiffs have had difficulty "in establishing that they have been damaged as the result of a data security breach").

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

81. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140–41 (9th Cir. 2010).

82. *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1051 (E.D. Mo. 2009). In *Amburgy*, the court stated that since the plaintiff conceded that he did not know whether his personal information had been compromised in the breach, the likelihood of identity theft was purely speculative and the injury was too abstract to confer standing. *Id.* at 1052.

83. *Whitmore v. Arkansas*, 495 U.S. 149, 161 (1990) ("It is not for [the] Court to employ untethered notions of what might be good public policy to expand our jurisdiction in an appealing case.").

84. CHEMERINSKY, *supra* note 26, at 60. One main theory underlying justiciability doctrines such as standing is to preserve the judiciary as the arbiter of cases or controversies. See generally Jonathan R. Siegel, *A Theory of Justiciability*, 86 TEX. L. REV. 73 (2007) (comparing public and private rights' views of the judiciary's role).

successfully alleging compensable damages.⁸⁵ Although alleging injury for the purposes of proving standing is similar, damages in tort must be more concrete to be compensable.⁸⁶ Negligent conduct is not actionable unless there is an “individual whose interests have suffered.”⁸⁷ Tort law typically does not allow recovery of damages for economic loss without some physical harm.⁸⁸ As a result, contract-based claims tend to find more success than tort claims against the company maintaining the database.⁸⁹ Even in the context of contract claims, although courts are somewhat reluctant to quantify the monetary value of increased risk of harm and emotional distress,⁹⁰ “individual[s] losses from

85. See, e.g., *Pisciotta*, 499 F.3d at 640 (finding standing yet dismissing for failure to allege damages recognized by governing substantive law); *Holmes v. Countrywide Fin. Corp.*, No. 5:08 CV 00205 R., 2012 WL 2873892, at *6 (W.D. Ky. July 12, 2012) (stating that “an increased threat of an injury that may never materialize cannot satisfy the injury requirement” for damages); *Hammond v. The Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *9–13 (S.D.N.Y. June 25, 2010) (declaring that the “[p]laintiffs’ alleged increased risk of identity theft is insufficient to support Plaintiffs’ substantive claims” of negligence, breach of fiduciary duty, breach of implied contract, or state consumer protection laws); *Amburgy*, 671 F. Supp. 2d at 1054 (deciding that an “increased risk of identity theft, the time spent to monitor credit and other accounts, the loss and compromise of personal information, the loss of exclusive control over such information, and invasion of privacy” were insufficient to allege a compensable injury); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009) (holding that, while plaintiffs met the requirement for standing based on increased risk of identity theft, state common law requires dismissal for failure to allege appreciable harm), *aff’d*, 380 F. App’x 689 (9th Cir. 2010); *Pinero v. Jackson Hewitt Tax Serv. Inc.*, 594 F. Supp. 2d 710, 716 (E.D. La. 2009) (holding that a plaintiff who fails to allege any financial losses cannot state a claim for negligence under Louisiana law and cannot recover for emotional damages without a physical injury); *Ponder v. Pfizer, Inc.*, 522 F. Supp. 2d 793, 798 (M.D. La. 2007) (noting that by failing to show that he suffered “any actual damages—that someone actually used the disclosed information to his detriment,” a plaintiff failed to state a theory of damages that is recoverable or recognized by law); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 497 (Me. 2010) (holding that time and effort is not recognized by Maine law as a compensable injury in a negligence claim).

86. See Bishop, *supra* note 11, at 10 (explaining that courts use a similar rationale in deciding standing and damages issues but noting that standing is a jurisdictional requirement that potentially has a lower threshold).

87. W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 30, at 165 (5th ed. 1984).

88. See Bishop, *supra* note 11, at 18. However, at least one jurisdiction has enacted a statutory exception to the traditional prohibition against purely economic damages in identity theft cases. See 815 ILL. COMP. STAT. ANN. 505/10a(a) (West 2008) (permitting recovery for economic loss in identity theft cases through the Illinois Consumer Protection and Deceptive Practices Act).

89. See Ambrose, Jr. et al., *supra* note 79, at 651–58 (comparing plaintiffs’ approaches to showing damages).

90. Stephen J. Rancourt, *Hacking, Theft, and Corporate Negligence: Making the Case for Mandatory Encryption of Personal Information*, 18 TEX. WESLEYAN L. REV. 183, 195 (2011) (noting that quantifying damages suffered “down to a specific monetary number” proves difficult for most plaintiffs bringing actions arising out of data breaches).

identity theft [that] are generally fixed to the time and money spent in repairing credit.”⁹¹

Further, when a consumer knows that his information has been exposed and used, at least one circuit has allowed for the recovery of expenditures on credit monitoring services.⁹² In those cases, the plaintiff will be required to show that there was a “reasonable basis for purchasing identity theft insurance to avoid further damage.”⁹³ As such, a growing trend appears to be developing—actual identity theft, or real or attempted unauthorized use of the personal information is “a prerequisite for a successful claim based on a mass data breach.”⁹⁴ These common law obstacles to a judicial remedy for data breaches force plaintiffs to file suit “on the thinnest of legal reeds that will rarely survive motions for summary judgment, if not motions to dismiss.”⁹⁵

C. The Lack of Federal Data Privacy Laws Leaves Service Providers and Consumers Unsure of Data Security Obligations and Any Available Remedies

It is no surprise that legislation and case law at the local, state, and federal levels have fallen behind innovations and advancements in technology. Congress has been slow to react to the challenges presented by new technology and has yet to enact comprehensive federal personal data security breach notice legislation.⁹⁶ Despite this reluctance, it should be noted that Congress has enacted laws that prohibit hacking into databases with personal information,⁹⁷ restrict wiretapping where contents of a communication are intercepted in real

91. Bishop, *supra* note 11, at n.70; see also Anita Ramasastry, *Data Insecurity: What Remedy Should Consumers Have when Companies Do Not Keep Their Data Safe?*, FINDLAW’S WRIT (March 6, 2006), <http://writ.news.findlaw.com/ramasatry/20060306.html> (arguing that legislation should be drafted to overcome the economic loss rule and provide a remedy for consumers in data security breach situations).

92. *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 166 (1st Cir. 2011).

93. *Id.*

94. Pinson, *supra* note 64, at 57.

95. Ian Ballon & Wendy Mantell, *Defending Data Privacy and Behavioral Advertising Putative Class Action Suits*, 1095 PLI/PAT 481, 485 (2012).

96. See Patricia E.M. Covington & Meghan S. Musselman, *Recent Privacy and Data Security Developments*, 65 BUS. LAW. 611, 612 (2010) (noting that with the new consumer financial protection agency, the federal government may be “positioning itself to regain prominence in the regulation of privacy and data security”); Carolyn A. Deverich, Brian R. Strange & David A. Holop, *Into the Breach: Plaintiffs Have Been Increasingly Successful in Gaining Injunctive Relief for Online Security Breaches*, 34 L.A. LAW 27, 30, 32 (2012) (explaining that the federal government has successfully passed data breach notification laws that affect some entities).

97. Consumer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2006 & Supp. 2012) (prohibiting (1) unauthorized access to the data involving national security; (2) intentional access of government computers; (3) knowingly accessing a protected computer with the intent to commit fraud; (4) unlawfully obtaining financial information from a government agency or from a computer in interstate commerce; (5) causing damage to computers; (6) trafficking passwords; and (7) threatening to cause damage to a computer through extortion).

time⁹⁸ or accessed in electronic storage,⁹⁹ regulate the collection, dissemination, and use of consumer information by credit reporting agencies,¹⁰⁰ and prohibit the disclosure of personal information kept by federal agencies without consent of the individual to whom the information pertains.¹⁰¹ In practice, however, commentators find that these federal statutes fail to adequately provide a remedy for consumers who fall victim to data security breaches.¹⁰² None of Congress's efforts have addressed data breaches that have not resulted in actual identity theft; instead, Congress requires plaintiffs to allege a minimum monetary damage amount to bring a civil action, which is often difficult for plaintiffs to meet.¹⁰³ Numerous comprehensive data privacy bills have been proposed in Congress, but none have found substantial support in either chamber.¹⁰⁴ In contrast, administrative agencies have begun to devote attention to the growing issue.¹⁰⁵

98. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2006 & Supp. 2012).

99. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006 & Supp. 2012).

100. Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* (2006)

101. Privacy Act of 1974, 5 U.S.C. § 552a (2006 & Supp. 2012); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006) (establishing guidelines for online management of personal information of children under the age of thirteen).

102. Ballon & Mantell, *supra* note 95, at 486 (discussing how the Electronic Communications Privacy Act requirement of “showing . . . unauthorized access to the *contents* of a communication” poses an obstacle for plaintiffs because personal information is not considered “contents” under the Act); *see, e.g.*, Hill v. MCI WorldCom Commc’n, 120 F. Supp. 2d 1194, 1195–96 (S.D. Iowa 2000) (holding that names, addresses, and phone numbers allegedly divulged were not considered by the court to fall within the statutory definition of “contents” under the Electronic Communications Privacy Act); Jessup-Morgan v. Am. Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that the Electronic Communications Privacy Act did not apply to AOL’s disclosure of information identifying an AOL electronic communication account because the disclosure was made to a private party rather than to a governmental entity).

103. *See, e.g.*, Consumer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(5)(B)(i) (2006) (requiring a minimum of \$5,000 in aggregate damages within a one year period to maintain a cause of action). This minimum damages requirement was later repealed. 18 U.S.C. § 103(a)(5) (Supp. 2012).

104. *See e.g.*, S. 1535, 112th Cong. (2011) (introduced on Sep. 8, 2011, and sent to the House or Senate for consideration on Sep. 22, 2011, with no further action); S. 1408, 112th Cong. (2011) (introduced on July 22, 2011, and the committees assigned to the bill sent it to the House or Senate as a whole for consideration on September 22, 2011, but no further action has been taken); H.R. 5318, 109th Cong. (2006) (introduced on May 9, 2006, but was not enacted); ; H.R. 4127, 109th Cong. (2005) (introduced on March 19, 2006, but was not enacted); H.R. 3997, 109th Cong. (2005) (introduced into Congress on March 16, 2006, but was not enacted); S. 1789, 109th Cong. (2005) (introduced on Sep. 19, 2005, but was not enacted); S. 1408, 109th Cong. (2005) (introduced on July 28, 2005, but not enacted); S. 1326, 109th Cong. (2005) (introduced but no roll call votes taken).

105. Rebecca S. Eisner et. al., *A Year in the Clouds: More Businesses Adopt Enterprise Cloud Computing Despite Privacy and Data Concerns*, in PRACTICING LAW INSTITUTE, CLOUD INNOVATION AND OTHER HOT TOPICS 177, 188–93 (discussing the FTC’s response to businesses’ adoption of new technology and data security).

The FTC and the recently created Consumer Financial Protection Bureau are the primary sources of federal consumer protection enforcement.¹⁰⁶ In 2010, the FTC released a suggested framework for businesses to use in assessing and implementing data privacy standards.¹⁰⁷ The FTC uses its authority to regulate unfair practices by pursuing companies that fail to take “reasonable and appropriate measures” to secure personal information.¹⁰⁸ By regulating businesses that aggregate consumer personal information, these government entities aim to protect the privacy of consumers who share this information with a service provider or business.¹⁰⁹

In addition to prohibiting unfair practices,¹¹⁰ the FTC relies heavily on the Gramm-Leach-Bliley Act to help ensure consumer privacy.¹¹¹ Under the Act, the FTC requires financial institutions to provide consumers with notice of a privacy policy.¹¹² The Act also requires financial institutions to implement a written safeguarding program that corresponds with the size, nature, complexity, and scope of the institution’s business.¹¹³

Despite these efforts, no federal statute or administrative action mandates absolute standards.¹¹⁴ Instead, businesses are forced to rely on guiding principles, including the limitation of network access, use of comprehensive security software, creation of strong passwords and data encryption, and curtailment of the storage of unnecessary data.¹¹⁵ Consequently, the key to avoiding liability for data breaches is to adopt privacy standards that are

106. See Press Release, Consumer Financial Protection Bureau, Federal Trade Commission Pledge to Work Together to Protect Consumers (Jan. 23, 2012), *available at* <http://www.ftc.gov/opa/2012/01/ftccfpb.shtm>.

107. See generally FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESS AND POLICYMAKERS (2010), *available at* <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

108. Covington & Musselman, *supra* note 96, at 613–15 (discussing recent FTC enforcement actions based on a claim of unfair practice).

109. Roland L. Trope & E. Michael Power, *Lessons in Data Governance: A Survey of Legal Developments in Data Management, Privacy and Security*, 61 BUS. LAW. 471, 504 (2005). Entities meeting the definition of a “financial institution” are required to: (1) identify at least one employee to coordinate a security program; (2) determine reasonably foreseeable risks to security of customer information; (3) design and implement a security program to control risks with regular procedure assessments; (4) contract with service providers that can maintain appropriate safeguards for consumer personal information and contractually require maintenance of these safeguards; and (5) evaluate and adjust procedures according to changes in circumstance. 16 C.F.R. § 314.4 (2012).

110. See Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2006); see *supra* note 108 and accompanying text.

111. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C.); Covington & Musselman, *supra* note 96, at 614–15.

112. 15 U.S.C. §§ 6803–6804 (2006).

113. *Id.*

114. Eisner et. al., *supra* note 105, at 545.

115. *Id.*

designed to prevent a breach before it occurs.¹¹⁶ Although many businesses are aware of the importance of such security measures, the lack of concrete federal guidance leaves businesses unsure of how to comply with data security rules.¹¹⁷

In contrast to the relative inactivity at the federal level, a majority of state legislatures have enacted data security measures reflecting the need to protect consumer privacy interests.¹¹⁸ State laws on data security largely focus on providing timely notification to consumers following a security breach.¹¹⁹ Notification requirements garner intense media attention and may create apprehension among consumers whose personal information is stored by a business experiencing a breach.¹²⁰ In addition to requiring notification in the event of a security breach, a select few states require businesses to implement proactive safeguards for data security.¹²¹ The statutes, however, are still

116. See Fernando M. Pinguelo, Wayne Lee & Bradford W. Muller, *Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships Are Attempting to Achieve for the Nation of Tomorrow*, 17 VA. J.L. & TECH. 75, 82 (2012). Advanced planning is essential such that “[i]n an emergency incident response situation, a well-written and properly socialized incident response plan will be the best method to inform the relevant stakeholders, identify the incident, and contain the security breach.” *Id.*

117. See Dort, *supra* note 11, at *8 (explaining that, in light of disclosure obligations, businesses often choose to comply with the most stringent statutes and provide the same information to all implicated individuals, regardless of the requirements in their state of residence).

118. See Covington & Musselman, *supra* note 96, at 617 (noting that forty-four states already had some type of security breach notification law in place prior to 2009, when legislation introduced in the House of Representatives made federal regulation a distinct possibility).

119. 2012 *Security Breach Legislation*, NAT’L CONFERENCE OF STATE LEGISLATURES (Dec. 13, 2012), <http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2012.aspx> (indicating that as of December 2012, forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted some form of statutory notification requirement to provide guidance in the event of a security breach that exposed personal information). Only Alabama, Kentucky, New Mexico, and South Dakota do not mandate notification following a security breach. See *State Security Breach Notification Laws*, NAT’L CONFERENCE OF STATE LEGISLATURES (Aug. 20, 2012), <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.

120. See Gonzalez, *supra* note 5, at 1355; Trope & Power, *supra* note 109, at 487 (quoting E. MICHAEL POWER & ROLAND L. TROPE, *SAILING IN DANGEROUS WATERS: A DIRECTOR’S GUIDE TO DATA GOVERNANCE* 301 (2005)). Of the two statutory schemes regarding notification, the more flexible model, used by California, does not require disclosure in every instance, providing a business with the opportunity to address a breach situation as it deems appropriate. See Trope & Power, *supra* note 109, at 488 (quoting *Data Breaches and Identity Theft: Prepared Statement of Fed. Trade Comm’n Before the S. Comm. on Commerce, Sci. and Transp.*, 109th Cong. 11–12 (2005) (statement of Deborah Platt Majoras, Chairman, Fed. Trade Comm’n)).

121. See, e.g., ARK. CODE ANN. § 4-110-104(b) (West 2011) (instructing businesses with access to personal information to implement security procedures); CAL. CIV. CODE § 1798.81.5(c) (West 2009) (mandating a business that maintains personal information to adopt reasonable security measures to protect data); MASS. GEN. LAWS ANN. ch. 93H, § 2(a) (West Supp. 2012) (requiring the drafting of regulations to “safeguard the personal information of

largely insufficient because they require notification only in certain circumstances, do not require data encryption, or do not provide a private cause of action.¹²² Inconsistencies among state statutes on businesses' pre- and post-breach duties result in confusion on how businesses should comply in an interstate context.¹²³

II. THE SPLIT IN CIRCUIT OPINIONS AND THE RELUCTANCE OF THE SUPREME COURT TO HEAR THE ISSUE LEAVE AN OPEN QUESTION WITH WHICH THE CIRCUIT COURTS MUST WRESTLE

The Supreme Court recently denied certiorari in *Reilly*, leaving unanswered questions on whether a consumer whose personal information has been exposed following a data breach has suffered an injury sufficient to confer standing in federal court.¹²⁴ With a lack of consensus among circuits and no clarification from the Supreme Court, district courts have struggled to reconcile settled standing jurisprudence with existing data security precedent.¹²⁵ As a result, clear guidance for future data breach suits is needed. Courts, however, are in a challenging position. If they find standing, they are arguably extending constitutional jurisdiction beyond its bounds, but reaching

residents of the [C]ommonwealth" of Massachusetts); NEV. REV. STAT. ANN. § 603A.210 (LexisNexis 2011) (providing instructions to destroy personal information when a business no longer needs the records); N.C. GEN. STAT. § 75-64 (2011) (directing businesses to develop preventative measures to protect against "unauthorized access" to personal information); OR. REV. STAT. § 646A.622 (West Supp. 2011) (requiring businesses to implement security measures to protect personal information); TEX. BUS. & COM. CODE ANN. § 521.052 (West 2011) (same).

122. See, e.g., Gonzalez, *supra* note 5, at 1365, 1368, 1370–71 (arguing that an Arizona data security statute fails to protect consumers because it only requires notification when the business anticipates material harm as a result of the security breach, conservatively defines "personal information" so that that some data is left unprotected, and does not allow consumers to seek retribution in a private action against the company at fault); see also *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 636–37 (7th Cir. 2007) (noting similar deficiencies in Indiana's data security statute, which mandates "only that a database owner *disclose* a security breach to potentially affected consumers," requiring no other action to mitigate the breach and foreclosing private causes of action).

123. See Pinson, *supra* note 64, at 62–63 (2007); see also Pinguelo et al., *supra* note 116, at 75 (advocating for cooperation between the public and private sectors in order to make sense of the varying jurisdictional approaches to regulating the prevention and mitigation of security breaches).

124. *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 46 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012).

125. See, e.g., *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1051 (E.D. Mo. 2009) (declining to adopt the rationale that the *Pisciotta* court used to find standing because it "engaged in no discussion applying the Supreme Court's recognized standard for determining whether plaintiffs in a database breach case had standing under Article III); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (citing *Pisciotta*'s failure to apply applicable case law in its determination that plaintiff lacked standing).

an outcome that is fair and just for consumers.¹²⁶ On the other hand, by denying standing in data breach suits, courts are likely conforming with the law, but hurting consumers and effectuating bad public policy.¹²⁷

A. Holding That an Increased Threat of Future Identity Theft Is Sufficient to Confer Article III Standing Stretches the Doctrine to Its Limits

If courts follow the approach taken by the Seventh and Ninth Circuits that an increased risk of identity theft is sufficient to establish standing, negligent businesses whose data is stolen would be held accountable in a court of law. Consequently, recognizing standing in this unique realm of putative class action suits would create an incentive for businesses to proactively minimize the dangers of security breaches.¹²⁸ On the other hand, by denying standing to plaintiffs in data breach suits who have not yet had their identity stolen, courts can avoid a merits determination on a technicality.¹²⁹ Precluding legal redress forces consumers to navigate the complex nature of modern database management without any standards against which to hold businesses or any redress for a failure to meet those standards.¹³⁰ The potential injustice resulting from the consumer bearing the responsibility of a business's negligent maintenance of personal information demonstrates the need for a mechanism under which a business shares in the liability.¹³¹

126. See *infra* Part II.A.

127. See *infra* Part II.B.

128. Dort, *supra* note 11, at *4 (explaining that businesses will take preventative measures to avoid litigation). Common steps towards minimizing security breaches include: “1. Securing a networked environment from within a comprehensive firewall and controlling access to the network; 2. Implementing external data security; 3. Installing networked security traps; 4. Applying system and personal identity verification protocols; 5. Implementing data encryption; [and] 6. installing intrusion detection systems . . .” *Id.*

129. See KLOPPENBERG, *supra* note 39, at 1, 14–15 (arguing that the Supreme Court routinely invokes the standing doctrine to avoid resolving disputes in more controversial cases, particularly cases with racial overtones).

130. See Pinguelo et al., *supra* note 116, at 80–84 (explaining the complex nature of cybercrimes and cybercriminals and the many steps a business should take to maintain the security of its information and prevent against a security breach); Bob Sullivan, *Study: ID Theft Usually an Inside Job*, NBCNEWS.COM (Mar. 21, 2004, 7:03:32 PM), <http://www.nbcnews.com/id/5015565/> (referring to the “painstakingly” difficult process of tracing the origin of an identity theft crime). Identity thieves intercept millions of pieces of personal information that can be used fraudulently in a number of ways. See *Chronology of Data Breaches Security Breaches 2005 – Present*, PRIVACY RIGHTS CLEARINGHOUSE (Mar. 19, 2013), <http://www.privacyrights.org/data-breach> (showing 607,280,163 records breached and 3,665 data breaches made public since 2005).

131. See Pinson, *supra* note 64, at 31–32 (identifying the types of personal information and the cost associated with a security breach and the growing trend, as evidenced by state data security legislation, of compelling businesses to guard against and bear the burden of a breach); Schneider, *supra* note 60, at 290–93 (proposing two measures: (1) recognizing a new type of injury that allows for recovery in a security breach; or (2) providing for a negligence cause of action by the state to hold businesses accountable for negligent management of consumer data);

In spite of consumer protection advocates' desire for an expansion of the definition of an injury in fact, courts have a duty to uphold the Constitution and respect the roles of the political branches of government.¹³² Article III requires that the federal judiciary only hear "cases" and "controversies."¹³³ Injury is not only required for a plaintiff to succeed on the merits of a claim,¹³⁴ but it is clear through standing jurisprudence that the failure to allege an actual injury is an absolute bar to accessing federal court.¹³⁵ The Supreme Court, as the final arbiter in the interpretation of the Constitution, often resists addressing the merits of a claim when standing is in dispute to avoid the perception that the judiciary is usurping the lawmaking authority of the legislature and the enforcement power of the executive branch.¹³⁶ However, the Court has historically expanded the standing doctrine to consider harms that might be more speculative, rather than concrete, in nature.¹³⁷ For example, the Court recognized standing when plaintiffs alleged that enjoyment of the environment could be diminished by the potential likelihood of decreased recycling caused by an increase in freight rates.¹³⁸ Yet, some courts have not recognized the irreparable damages to financial reputations and freedoms of consumers caused by data breaches as sufficient injury for standing.¹³⁹

However, even if the courts grant standing, it is unlikely that a consumer will be able to allege compensable injury for purposes of determining a

Blades, *supra* note 11, at 526 (suggesting that businesses should bear the cost of credit monitoring to "prevent the injustice of requiring the economically disadvantaged consumer from paying fees caused by the [business's] negligence").

132. See *Allen v. Wright*, 468 U.S. 737, 752 (1984) (describing standing as a principle "built on a single basic idea – the idea of separation of powers"); see also *THE FEDERALIST* NO. 48, at 279 (James Madison) (Clinton Rossiter ed., Seven Treasures Publications 2008) (stating that "[a]fter discriminating . . . the several classes of power . . . the next and most difficult task is to provide some practical security for each, against the invasion of the others. What this security ought to be, is the great problem to be solved.").

133. U.S. CONST. art. III, § 2.

134. See *supra* notes 86–93 and accompanying text.

135. See *supra* notes 41–49 and accompanying text.

136. *CHEMERINSKY*, *supra* note 26, at 60.

137. See, e.g., *Massachusetts v. Env'tl. Prot. Agency*, 549 U.S. 497, 516–26 (2007) (finding that the state of Massachusetts had standing to sue the Environmental Protection Agency because the state has an interest in the coastal lands lost by rising water levels, even in the absence of a visible claim by an individual harmed by greenhouse gases); *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 686–87 (1973) (holding that students who claimed their enjoyment of forests, streams, and mountains would be diminished had shown sufficient harm to meet Article III standing requirements).

138. *Students Challenging Regulatory Agency Procedures*, 412 U.S. at 675–76.

139. See Robert Terenzi, Jr., Note, *When Cows Fly: Expanding Cognizable Injury-in-Fact and Interest Group Litigation*, 78 *FORDHAM L. REV.* 1559, 1604 (2009) (discussing the need to include potential future injuries in the scope of the injury requirement). A 2007 study by the Identity Theft Resource Center found that seventy percent of identity theft victims require up to a year to resolve issues caused by identity theft, while almost twenty percent of victims need two or more years to resolve any credit issues. *IDENTITY THEFT RESOURCE CTR.*, *supra* note 8, at tbl. 9.

damage award.¹⁴⁰ An additional exception to the traditional common law rule requiring non-economic harm to successfully allege damages in a negligence claim would also be required.¹⁴¹ Just as with standing, courts are historically reluctant to create new causes of action, and prefer to leave that task to the legislature.¹⁴²

As a matter of public policy, however, businesses, who are in a better position to avoid data security breaches, should be held accountable for their negligence.¹⁴³ Ensuring that consumers have some judicial remedy for a business's careless database management would save the consumer from bearing the costs associated with the aftermath.¹⁴⁴

B. Alternatively, Holding That an Increased Risk of Identity Theft is Too Speculative or Conjectural to Confer Article III Standing Comports with Recognized Standing Jurisprudence, But at the Detriment to Consumers

A determination that an increased risk of identity theft is too speculative or conjectural to confer Article III standing in data security breach suits could assure businesses that they will not face a flood of federal class action suits in the aftermath of a security breach, regardless of whether the breach was due to the negligence of the database manager.¹⁴⁵ Since federal courts are courts of limited jurisdiction that can only hear cases or controversies within

140. See e.g., *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 639–40 (7th Cir. 2007) (finding standing yet dismissing a suit for failure to allege damages recognized by the governing substantive law); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009) (stating that, while a plaintiff may meet the standing requirement based on an increased risk of identity theft, state common law may require dismissal of the claim for failure to allege appreciable harm), *aff'd*, 380 F. App'x 689 (9th Cir. 2010); *In re Hannaford Bros. Co. Customer Data Security Breach Litig.*, 4 A.3d 492, 496 (Me. 2010) (holding that time and effort is not usually recognized by Maine case law as a compensable injury in a negligence claim).

141. See e.g., *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162 (1st Cir. 2011) (mitigating plaintiffs' costs by finding that purchasing identity theft insurance was reasonable to avoid further economic damage when a third party had conducted unauthorized transactions using the plaintiff's information).

142. See *Pisciotta*, 499 F.3d at 637 (deferring to the legislature's intent and refusing to recognize credit monitoring costs as compensable damages because, "[h]ad the . . . legislature intended that a cause of action should be available . . . for failing to protect adequately personal information, we believe that it would have made some more definite statement of that intent").

143. For example, the database manager can more easily monitor database security. Since businesses are the entities with which consumers entrust their personal information, it logically follows that the businesses should be charged with protecting consumer information.

144. Costs might include lost time, money, and security. Consumers often close potentially compromised accounts, purchase credit monitoring services, spend time monitoring their accounts themselves, and experience increased stress and worry as a result of the breach. See IDENTITY THEFT RESOURCE CTR., *supra* note 8, at 2–4.

145. Since standing is a jurisdictional hurdle that can be addressed sua sponte, a Supreme Court decision declaring that breach victims lack standing provides concrete precedent for dismissal. See *supra* note 47 and accompanying text.

constitutional limits, a court may not consider the merits of a case if it determines that the plaintiff does not have standing.¹⁴⁶

By refusing to expand the standing doctrine's injury analysis to include increased risk of future harm, the courts reaffirm the principle that the alleged injury must be concrete and particularized to the plaintiff.¹⁴⁷ This determination also serves the guiding twin rationales behind the doctrine: separation of powers and judicial efficiency.¹⁴⁸ But, as many commentators have suggested, consideration of injury for standing purposes inherently implicates weighing the merits of the claim.¹⁴⁹ However, considering the double hurdle faced by plaintiffs in data breach suits, it is unlikely that the judiciary will risk its reputation as the non-political branch¹⁵⁰ by expanding the realm of standing and classification of compensable damages in order to permit consumers an avenue for relief.¹⁵¹

C. Congress Could Pass Much Needed Comprehensive Data Privacy Legislation to Resolve Uncertain Obligations of Service Providers and Provide Remedies to Consumers After a Data Security Breach

Congress can minimize the hurdle faced by plaintiffs in data security breach suits. By creating a private cause of action specifically delineating affected parties as the proper parties to bring suit,¹⁵² Congress can provide a statutory solution to the problem facing consumers when attempting to assert their claims in federal court. Clearly articulating its intent to confer a right to sue to affected parties in the legislative history could permit Congress to effectively resolve the issue for consumers without the statute being found unconstitutional. An act of Congress would also resolve inconsistencies between varying state statutes.

The lack of uniformity in state laws governing data management and security breach notification leaves businesses, especially those doing business nationally, struggling to comply with forty-six individual laws, each imposing

146. U.S. CONST. art. III, § 2.

147. See *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

148. See CHEMERINSKY, *supra* note 26, at 59–60.

149. See KLOPPENBERG, *supra* note 39, at 39–42 (articulating that standing is often used by courts to avoid making decisions based on the merits of the claim due to a technicality); Nichol, Jr., *supra* note 39, at 636–37 (disapproving of the Court's application of the standing doctrine in reaching a decision); Tushnet, *supra* note 39, at 664 (criticizing the use of standing as a way for courts to avoid difficult claims and proposing abolishing the current jurisprudence).

150. *United Pub. Workers v. Mitchell*, 330 U.S. 75, 90–91 (1947) (articulating the fear that “[s]hould the courts seek to expand their power so as to bring under their jurisdiction ill-defined controversies over constitutional issues, they would become the organs of political theories . . . and would properly meet rebuke and restriction from other branches” of government).

151. FED. R. CIV. P. 12(b)(6).

152. See *supra* notes 53–55 and accompanying text (discussing statutory standing).

different obligations and providing varying remedies.¹⁵³ Federal laws governing privacy have proven difficult to apply to data security breaches due to narrow definitions and the unique nature of modern data management.¹⁵⁴ Regulatory guidance by the FTC has provided some assistance in compliance,¹⁵⁵ but the general deficiencies of explicit federal direction have forced businesses to self regulate, thereby placing consumers at the mercy of the marketplace.¹⁵⁶ Since the Internet has created a global exchange of information that crosses state and international boundaries, Congress should intervene by providing comprehensive data management standards and remedies for consumers harmed by negligent data management.

Congress crafted a legislative solution to a similar, albeit different, problem when it enacted the Telephone Consumer Protection Act of 1991 (TCPA) to protect consumers from telephone abuses.¹⁵⁷ In addition to authorizing the Federal Communications Commission to promulgate regulations implementing the statute, the TCPA, a strict liability statute, gave consumers a private cause of action against violators.¹⁵⁸ The TCPA has proven to be an effective enforcement mechanism, with consumers bringing successful suits against alleged violators.¹⁵⁹ Consumer success in bringing and prevailing in TCPA

153. See, e.g., CAL. CIV. CODE. §§ 1798.80–84 (West 2009 & Supp. 2013) (imposing data protection obligations and authorizing suits for damages from breach of the duty to maintain data security); COLO. REV. STAT. § 6-1-716(4) (2012) (disallowing private causes of action for consumers impacted by a data breach); FLA. STAT. ANN. § 817.5681 (West 2006) (imposing only civil penalties for failure to maintain data security).

154. See Ballon & Mantell, *supra* note 95, at 486 (discussing how the Electronic Communications Privacy Act (ECPA) requirement of “showing . . . an unauthorized access to the contents of a communication” poses an obstacle for plaintiffs because personal information is not considered “contents” under the ECPA); see e.g., Hill v. MCI WorldCom Commc’n, 120 F. Supp. 2d 1194, 1196 (S.D. Iowa 2000) (dismissing the plaintiff’s complaint because it could not support a finding that MCI disclosed information that satisfied the ECPA definition of “content”); Jessup-Morgan v. Am. Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (finding that definitions of the ECPA, as written, made the Act inapplicable to subpoenas for communications information).

155. See Dort, *supra* note 11, at *5–6 (noting that the Gramm-Leach-Bliley Act “requires the FTC . . . to issue regulations ensuring that financial institutions protect the privacy and security of customer financial information”).

156. Eisner et al., *supra* note 105, at 185–86.

157. Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2006 & Supp. 2011). The TCPA prohibits a variety of practices ranging from unsolicited facsimile advertisements to the use of automatic telephone dialing systems and prerecorded messages. 47 U.S.C. § 227(b)(1). For a detailed discussion about how private enforcement of public laws is beneficial to private parties and helps supplement public enforcement, see J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137 (2012). Private enforcement mechanisms have seen some success in deterring behavior alongside traditional civil and criminal penalties brought on by governmental entities. *Id.* at 1153–58.

158. 47 U.S.C. § 227(b)(3).

159. See Paul Karlsgodt, *Battleground TCPA*, CLASSACTIONBLAWG.COM (Oct. 20, 2011), <http://classactionblawg.com/2011/10/20/battleground-tcpa/> (noting that class action suits are

suits provides support for the idea that Congress should create an effective and useful remedial tool for consumers affected by data breaches.

III. CONGRESS SHOULD PASS COMPREHENSIVE DATA PRIVACY LEGISLATION TO RESOLVE THE ISSUE FOR BUSINESSES AND CONSUMERS

It is unlikely that, absent any state or federal statute, courts will be persuaded that data security breaches and the resulting increased risk of identity theft are a sufficient basis to establish standing.¹⁶⁰ By deferring the authority to create a private cause of action to Congress or state legislatures, the judiciary stays within its proper role in the American system of government.¹⁶¹ Congress is the most appropriate branch to resolve any issues arising from novel concepts of law. Further, while enforcement may be pursued through the FTC or another qualified regulatory agency, it is the duty of Congress to make the laws.¹⁶²

Congress's constitutional authority to pass comprehensive data privacy legislation arises under the Commerce Clause, which is used to pass statutes that regulate interstate commerce.¹⁶³ By passing federal data privacy legislation that preempts state law, Congress would provide businesses serving consumers nationwide legal certainty as to which law applies.¹⁶⁴ While there have been many legislative proposals to resolve the lack of clarity in data privacy, none have gained sufficient support to become law.¹⁶⁵ Due to the

increasing in prevalence under the private cause of action created by the TCPA, particularly alleged violations of the prohibition on unsolicited facsimile advertisements).

160. See *supra* Part I.B.

161. See *supra* notes 30–33, 84 and accompanying text (discussing separation of powers as a primary reason for the standing doctrine).

162. U.S. CONST. art. I.

163. U.S. CONST. art. I, § 8, cl. 3. Congress has the authority “[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian tribes.” *Id.*; see *Gonzales v. Raich*, 545 U.S. 1, 16–17, 22 (2005) (finding that in the aggregate, marijuana grown for personal consumption intrastate has a substantial effect on interstate commerce, and, therefore, can be regulated by Congress); *United States v. Lopez*, 514 U.S. 549, 561–63 (1995) (holding that possession of a gun near a school is not an economic activity that has a substantial effect on interstate commerce and, therefore, is not within Congress's Commerce Clause powers); *Katzenbach v. McClung*, 379 U.S. 294, 301–04 (1964) (holding that Congress was within its power under the Commerce Clause to forbid restaurants from discriminating against racial minorities based on the rationale that interstate travelers and serving food crossed state lines); *Heart of Atlanta Motel v. United States*, 379 U.S. 241, 255–58 (1964) (holding that Congress could prohibit discrimination in public accommodations pursuant to the Commerce Clause); *Wickard v. Filburn*, 317 U.S. 111, 127–29 (1942) (finding that intrastate wheat production could be regulated by the Agricultural Adjustment Act because it had a substantial effect on interstate wheat demand); *Gibbons v. Ogden*, 22 U.S. 1, 19–21 (1824) (stating that Congress has the power to regulate interstate commerce that includes regulation of navigable waterways).

164. See *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1056–57 (E.D. Mo. 2009) (demonstrating that confusion can arise as to which state's data privacy law governs in a class action suit).

165. See *supra* note 104 (collecting a number of congressional proposals beginning in 2005).

complexity of the issue, it has been nearly impossible for Congress to account for various circumstances and protections needed.¹⁶⁶ In order to resolve the standing and damages issues presented in this novel area of law, a complex statutory structure that provides a private cause of action, imposes penalties for noncompliance, requires notification in all instances of data security breaches, permits recovery of civil damages by consumers, and authorizes the FTC to promulgate regulatory details is essential.

A. Congress Should Authorize the FTC to Establish Minimum Standards of Data Management and Impose Civil Penalties for Noncompliance

One failure of the state data security statutes is the lack of standards required for data management.¹⁶⁷ The FTC has proposed generic guidelines of basic precautions to protect consumers' personal information, but the agency does not currently have authority to promulgate official regulations.¹⁶⁸ Congress can inhibit unauthorized, third parties from extracting personal information, such as social security numbers, by authorizing the FTC to impose regulations that require encryption of all consumer information stored in a database.¹⁶⁹ If Congress makes the demand for universal encryption of data through statutory authorization to the FTC, the FTC can promulgate rules and regulations that require encryption based on the size of the business and the type of personal information stored. By requiring encryption of personal identification and account information that is stored or in transit, the FTC can tailor regulations by balancing expenses to the business and consumer protection interests with the overall public policy goal of preventing future litigation.¹⁷⁰ In addition, because a large number of data security breaches occur due to negligent database management, Congress should impose stringent standards for firewall protection.¹⁷¹ Such firewall standards can also be considered and promulgated by the FTC.¹⁷²

166. Congress sometimes authorizes independent departments and agencies to promulgate the specific implementation details because they are better placed to account for business and consumer concerns through the rulemaking process. See Pinguelo et al. *supra* note 116, at 86.

167. See Gonzalez, *supra* note 5, at 1373 (discussing Arizona's statute).

168. See FED. TRADE COMM'N, *supra* note 107, at iv–vii.

169. See Rancourt, *supra* note 90, at 214 (encouraging the use of mandatory encryption for data in transmission and storage).

170. J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI L. REV. 109, 127–29, 132–33 (2008) (detailing the FTC's current attempts to address data security and consumer personal information); Deverich et al. *supra* note 96, at 27–28.

171. A firewall is a software or hardware-based method to keep networks secure. Rolf Oppliger, *Internet Security: Firewalls and Beyond*, 40 COMM. OF THE ACM 92, 94 (1997). A firewall controls the incoming and outgoing network traffic by analyzing data packets and determining whether the packets analyzed should be permitted into the network. *Id.*

172. See Rancourt, *supra* note 90, at 214.

Large penalties should be set for failure to comply with the regulations in order to deter noncompliance.¹⁷³ The federal statute should impose a daily penalty to be collected and enforced by the FTC of \$1,000 when information is left unencrypted, and a \$5,000 daily penalty when unencrypted information is knowingly or willingly exposed to an unauthorized third-party.¹⁷⁴ Finally, the statute should impose a daily \$10,000 penalty when leaving information unencrypted ultimately results in identity theft in at least one case. This step-rate structure of penalties incentivizes business compliance due to the uncertainty of whether identity theft will actually occur.¹⁷⁵ Requiring minimum industry standards of data encryption allows businesses to formulate and adopt data management procedures that best fit each individual business, while penalizing noncompliance ensures that businesses will encrypt data to avoid fines.¹⁷⁶

173. See FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT: A REPORT TO CONGRESS 1 (2007), available at http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf (articulating the FTC's report to Congress in which it stated that civil penalties should grow increasingly larger to deter unlawful conduct).

174. See 47 U.S.C. § 227 (2006) (illustrating a similar penalty structure for knowingly or willingly violating the TCPA). The TCPA has been effective with minimal statutory damages of \$500. *Id.* In comparison, the ECPA permits statutory damages for wiretapping offenses in the amount of \$100 per day, up to \$10,000. 18 U.S.C. § 2520 (C) (2) (2006). The Fair and Accurate Credit Transactions Act, a statute requiring retailers to redact an individual's credit card number and expiration date from a transaction receipt, allows for damages from \$100.00 to \$1,000 per violation. 15 U.S.C. § 1681n (a)(1)(A) (2006). The addition of a penalty with no connection to the number of consumers affected, collected separate from the statutory damages recoverable by plaintiffs, would provide an additional incentive for businesses to comply regardless of any civil litigation that might arise.

175. See Brendan St. Amant, Recent Development, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 520 (2007) (stating that only two percent of those affected by data breaches are victims of related fraud). Because the motives of those perpetrating the data breach are often unknown, it is difficult to predict which breaches will result in fraud. See *id.* at 522–23 n.141 (citing *Data Security: The Discussion Draft of Data Protection Legislation*, Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 109th Cong. 29, 29–30 (2005) (statement by Chris Hoofnagle, Dir. and Senior Counsel, Electronic Privacy Information Center)). Such uncertainty regarding the risks of and circumstances leading up to the breach, as well as the serious and sometimes permanent effects of a breach, help to illustrate the importance and appropriateness of a deterrent penalty, the goals of which is to “impose a cost on wrongdoers that promotes compliance with the law.” Kenneth Mann, *Punitive Civil Sanctions: The Middleground Between Criminal and Civil Law*, 101 YALE L.J. 1795, 1830 (1992).

176. Mann, *supra* note 175, at 1831; see also Trope & Power, *supra* note 109, at 488 (discussing the flexibility available with similar minimum industry standards).

B. Congress Should Require Consumer Notification in the Event of a Data Breach in All Situations

The widespread proliferation of state-level data breach notification statutes illustrates their perceived effectiveness.¹⁷⁷ Some states impose a qualified notification requirement, only mandating disclosure in certain circumstances, such as when the stolen data was unencrypted.¹⁷⁸ However, a statute requiring notification, regardless of encryption, best serves the interests of consumers by providing an additional incentive for businesses to actively protect consumer information.¹⁷⁹ Although “over-notification may desensitize consumers to identity theft,”¹⁸⁰ these notification requirements would not cover situations in which a person lawfully accesses, but improperly uses, a consumer’s personal information.¹⁸¹ Thus, requiring notification in all instances of mass data breach in which personal information, such as social security and credit card numbers, dates of birth, names, and addresses, has been exposed best serves the interests of all parties by providing businesses with an incentive to comply and a standard with which to meet and giving consumers assurance that they will be notified in the occurrence of a breach.¹⁸²

C. Congress Should Create a Private Cause of Action, But Should Limit Damages to Credit Monitoring Service Expenditures and Attorneys Fees

As this Comment has discussed, plaintiffs in data security breach suits face an uphill battle to a judicial remedy.¹⁸³ Some state statutes allow for governmental enforcement but do not allow consumers to bring civil suits.¹⁸⁴ Creating a statutory cause of action, coupled with a federal enforcement

177. See NAT’L CONF. OF STATE LEGISLATURES, *supra* note 119 (indicating that at least forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have codified data breach notification requirements).

178. See, e.g., ARIZ. REV. STAT. § 44-7501 (Supp. 2012) (only requiring notification in the event of a security breach involving unencrypted data).

179. See Brandon Faulkner, *Hacking into Data Breach Notification Laws*, 59 FLA. L. REV. 1097, 1104, 1100 (2007) (stating that the traditional deterrent of civil litigation has seemingly failed to deter companies from acting negligently when securing their consumers’ personal information).

180. Gonzalez, *supra* note 5, at 1370.

181. See Sullivan, *supra* note 130.

182. See Gonzalez, *supra* note 5, at 1365–66; see also Faulkner, *supra* note 179, at 1114 (arguing that a “preemptive, federal breach notification statute” can eliminate the added transactional costs required by a company attempting to comply with various jurisdictions’ individual notification statutes). Faulkner also highlights that differences between states include the definition of personal identification information, when the notification is triggered, and what qualifies as timely notification. *Id.* at 1104.

183. See *supra* Part I.B.

184. *Supra* note 17 and accompanying text.

mechanism, would resolve the standing hurdle.¹⁸⁵ Further, in order to assuage plaintiffs' challenge in establishing damages, Congress should recognize that credit-monitoring services that are purchased as a direct result of a data breach notification represent a compensable injury.¹⁸⁶

Such a provision would not automatically cause a flood of litigation following a mass security breach because plaintiffs will still need to show the business's failure to comply with the set statutory requirements for data security. Additionally, imposing a recovery limit of \$1,000 per plaintiff¹⁸⁷ would check potentially speculative damage awards while still allowing consumers to recover for credit-monitoring services employed during the years immediately following the data breach.¹⁸⁸ Since this damage award is not automatic, a plaintiff will need to invest his or her time and money to bring a civil suit, which will further help to limit litigation to plaintiffs with significant personal interest in the matter. Further, because fewer than twenty percent of consumers affected by a data breach purchase credit monitoring services as a result of the breach, the number of litigants would be limited.¹⁸⁹ These safeguards ensure that plaintiffs will not assert broad and unfounded claims based on a hypothetical fear of identity theft and guarantees that recovery is limited to actual expenses incurred by a plaintiff because of a business's noncompliance with regulatory standards for data security management.

IV. CONCLUSION

The Supreme Court's wavering standing jurisprudence has resulted in inconsistent interpretations as to what constitutes a personally suffered injury.¹⁹⁰ Lower courts are therefore without guidance when applying the standing doctrine to novel questions of law provoked by new technologies. Federal courts are split in deciding whether sufficient injury has incurred for standing purposes when consumers' personal information has been exposed to

185. *Warth v. Seldin*, 422 U.S. 490, 514 (1975), *superseded by statute*, 33 U.S.C. § 1365(a) (2006), *as recognized in* *Mylonakis v. Georgios*, No. H-10-3031, 2012 U.S. Dist. LEXIS 171649, at *65–67 (S.D. Tex. Dec. 3, 2012).

186. See 47 § U.S.C. 227(b)(3) (2006) (illustrating an analogous action damages allowance).

187. *Debunking the Hype over ID Theft: You Don't Need a Costly Service to Protect Your Good Name*, CONSUMER REPORTS MONEY ADVISOR (Feb. 2012), <http://www.consumerreports.org/cro/2012/02/debunking-the-hype-over-id-theft/index.htm> (discussing identity theft protection, which averages between \$120 and \$300 annually); *Identity Theft Protection Services Review*, TOPTENREVIEWS.COM, <http://identity-theft-protection-services-review.toptenreviews.com/> (last visited Mar. 19, 2013) (comparing identity-theft protection services products offered in the marketplace).

188. PONEMON INST., 2012 CONSUMER STUDY ON DATA BREACH NOTIFICATION 1 (2012), *available at* <http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf> (stating that mass data breaches resulted in “some level of concern” for eighty-eight percent of affected customers).

189. *Id.* at 24.

190. See *supra* notes 36–59 and accompanying text.

an unauthorized third-party but has not yet been used fraudulently. Some courts consider the increased likelihood of future identity theft as a sufficient injury, while others consider this harm too speculative. Even after a court has found standing, however, plaintiffs still face the challenging task of alleging compensable injuries to recover damages. To avoid encroachment of the judiciary into the law-making function of the legislature and the law enforcement function of the executive, Congress should adopt comprehensive data privacy legislation. An effective legislative scheme would impose national minimum standards for data security procedures and penalties for non-compliance. In addition, the statute would demand notification in all instances of data security breach. Lastly, and perhaps most importantly to consumers, the statute would permit a limited civil damages recovery to plaintiffs who purchased credit monitoring services as a result of the breach in security. Novel issues of law often test the separation of powers between the branches of government, and now data privacy should have its place on the congressional to-do list.