WHERE VICTIMS OF DATA BREACH STAND: WHY THE BREACH OF PERSONALLY IDENTIFYING INFORMATION SHOULD BE FEDERALLY CODIFIED AS SUFFICIENT STANDING FOR DATA BREACH CAUSES OF ACTION♦

INTRODUCTION

In today's technology-driven world, it is commonplace for consumers to give various companies their personal information and allow them to store their personal data online. The unintended effect of such a practice is the exponentially increased risk of high-profile hacks.[1] The worries of modern-day consumers are no longer limited to the literal theft of a laptop containing personal information—in 2017 alone, cyber

[1] Nick Wells, *How the Yahoo hack stacks up to previous data breaches*, CNBC (Oct. 4, 2017, 12:25 PM), https://www.cnbc.com/2017/10/04/how-the-yahoo-hack-stacks-up-to-previous-data-breaches.html [https://perma.cc/2LQQ-Q3G2].

hacks of consumer data stored in online databases made up more than half of the year's reported data breaches.[2] Some of the worst data breaches in history, in terms of the amount of information compromised and the resulting costs, have occurred in just the last few years.[3]

The largest documented data breach in history targeted Yahoo in 2013, which compromised three billion Yahoo users' accounts.[4] The hackers obtained access to names, email addresses, encrypted passwords, birth dates, telephone numbers, and answers to security questions.[5] The information breached from Yahoo was considered especially critical, as it enabled hackers to access Yahoo users' "connections to their banks, social media profiles, other financial services and users' friends and family."[6] Another staggering breach took place in 2017, affecting Equifax, a notable credit reporting agency that conducts credit checks that are relied on by many industries.[7] The hackers gained access to consumers' social security numbers, names, and birth dates.[8] Over 143 million Equifax consumers' identities were breached and, as a result, put at risk of misuse, while at least several hundred thousand identities were, in fact, misused.[9] For the purposes of this Note, the term "breach" will be used to refer to a situation where a consumer's personally identifying information was stolen by hackers but has not yet been used in a

[2] *Id.*; *see 2017 Annual Data Breach Year-End Review*, ITRC, https://www.idtheftcenter.org 2017-data-breaches/ [https://perma.cc/86U3-EHUX] ("The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, according to the 2017 Data Breach Year-End Review released by the Identity Theft Resource Center® (ITRC) and CyberScout®. The Review indicates a drastic upturn of 44.7 percent increase over the record high figures reported for 2016."); *see also* Yiyi Miao, *11 of the Largest Data Breaches of All Time [Updated]*, OPSWAT (Nov. 22, 2017), https://www.opswat.com/blog/11-largest-data-breaches-all-time-updated [https://perma.cc/HG9V-TYUA] ("There were 8,069 data breaches between January 2005 and November 2017 according to the Identity Theft Resource Center, and in recent years the number of data breaches and compromised records has skyrocketed.").

[3] Miao, *supra* note 2.

[4] Wells, *supra* note 1.

[5] Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html [https://perma.cc/39KH-HVDQ].

[6] *Id.*; *see* Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 80 (2017), http://jlsp.law.columbia.edu/wp-content/uploads/sites/8/2017/11/51-Lorio.pdf [https://perma.cc/7DYN-S7AG] ("Because individuals often use the same email address, password, and security questions for multiple Internet accounts, the third party hacker could potentially gain access to additional private accounts, including financial accounts, of 500 million individuals." (internal footnote omitted)).

[7] Miao, *supra* note 2.

[8] Adam Shell, *Equifax data breach could create lifelong identity theft threat*, USA TODAY (Sept. 9, 2017, 7:00 AM), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/ [https://perma.cc/E5LX-WQRZ].

[9] *Id.*; *see* Miao, *supra* note 2 ("In 2017, credit bureau Equifax was breached, putting the data of over 143 million Americans and many people in other countries at risk. At the very least, several hundred thousand identities were stolen. Although Equifax did not announce the breach until September 7, the breach took place several months prior, in May 2017. Hackers were able to breach Equifax by exploiting a vulnerability in open-source software Apache Struts . . . .").

fraudulent way; the term "misuse" will reflect an instance where a consumer's personally identifying information was stolen and used for identity theft or other such fraudulent uses.

The Yahoo and Equifax data breaches are only two of many detrimental data breaches in recent history.[10] This signals an obvious need to address this growing problem as consumers continue to digitally store more personal information,[11] and especially as hackers become more sophisticated.[12] The problem that arises when hackers obtain such sensitive data, even if it is not immediately misused, is that the data is "perpetually valuable."[13] Once hackers have obtained the data, it permanently remains in their possession as a mechanism for causing harm.[14] Following a breach, affected consumers are left vulnerable to the possibility that hackers will use their information for fraudulent purposes. For example, hackers may file tax returns, claim tax refunds, file fraudulent medical expense claims, open credit cards, rent an apartment, obtain loans, or buy houses in a victim's name—all without the victim knowing.[15] Not only can the consequences of such misuse be financially devastating, but it could also lead to the arrest and prosecution of innocent victims of the breach should their stolen information be used to commit fraud.[16] Given the expansive scope and serious nature of the risk that data breaches pose to innocent consumers, it is unsettling that legal remedies are not readily available to compensate victims.[17] It is particularly troubling that data breach victims are often denied their day in court to seek those legal remedies.

---

10 Miao, *supra* note 2.

11 Lorio, *supra* note 6, at 81.

12 Herb Weisbaum, *Hackers scored more Social Security numbers than stolen credit card numbers in 2017*, NBC NEWS (Feb. 21, 2018, 9:57 AM) (statement of Al Pascual), https://www.nbcnews.com/tech/security/smarter-criminals-find-new-ways-commit-cyber-fraud-n849691 [https://perma.cc/J5ME-9Q7R] ("Al Pascual, Javelin's research director and head of fraud and security, expects 2018 to be another record year for identity fraud because thieves have adapted to new security measures. 'They're smarter now. They have all the data they need to commit fraud and they know exactly how to use it . . . . They're getting more sophisticated faster than we can respond – and that's the big problem.'").

13 Shell, *supra* note 8.

14 *Id.* (statement of John Ulzheimer) ("This information is perpetually valuable. You are not going to change your name or date of birth or Social Security number. In five years they will be the same, unlike a credit card that takes five minutes to cancel over the phone.").

15 *Id.* ("Armed with your digital history, hackers can file tax returns using your name and [S]ocial [S]ecurity number to claim a refund. Or file fraudulent medical expense claims. Or attempt to open credit cards, rent an apartment, apply for electric service or get a loan and buy a house in your name without you knowing.").

16 Amul Kalia & Cindy Cohn, *Will the Equifax Data Breach Finally Spur the Courts (and Lawmakers) to Recognize Data Harms?*, EFF (Sept. 26, 2017), https://www.eff.org/deeplinks/2017/09/will-equifax-data-breach-finally-spur-courts-and-lawmakers-recognize-data-harms [https://perma.cc/ZV2Z-9LTE].

17 *Id*.

In the wake of a data breach, individuals who have experienced misuse, as well as those who have been put at risk of misuse, often turn to courts in an attempt to sue the companies that failed to protect their personal information and left it thus vulnerable to the efforts of hackers. Data breach cases, which often take the form of class actions, are generally litigated in federal court.[18] A plaintiff must therefore have Article III standing to sue, which requires the asserted injury meet a certain threshold, be directly caused by the defendant's conduct, and likely be curable by a favorable decision.[19] Importantly, the plaintiff's alleged injury must first meet a certain threshold to pass constitutional muster.[20] A plaintiff lacks constitutional standing, and is thus barred from pursuing a federal lawsuit, if they fail to show that the injury suffered is actual or imminent, as well as concrete and particularized.[21]

The ability of data breach victims to litigate in federal court often turns on the magnitude of the injury alleged. Deciding whether a data breach plaintiff has alleged the requisite injury-in-fact is a contentious issue that both Congress and the Supreme Court have yet to address. Earlier this year, the Supreme Court declined to review *Attias v. Carefirst*,[22] a case that presented an opportunity to create a uniform test for claimant standing in data breach cases or, at the very least, to comment on the issue. This lack of guidance from the legislative and judicial branches has served to maintain a precedential split among the federal circuit courts as to what constitutes an injury in the data breach context[23] and has led to a bewildering patchwork of state data breach laws.[24]

As to the circuit split, some courts strictly apply the standing inquiry and hold that an alleged substantial risk of future harm following a data breach, without proof of misuse, does not amount to an Article III injury. "These courts mistakenly require actual or imminent loss of money due to the misuse of information that is directly traceable to a single breach."[25] Other courts hold that an alleged risk of future harm flowing from hackers' mere access to the plaintiff's personal information is sufficient to establish an Article III injury, even absent proof of misuse. These courts recognize the harm inherent in the breach of personally identifying

18 *See* discussion *infra* Part I; *see generally* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).
19 *Lujan*, 504 U.S. at 560-61.
20 *Id*. at 560.
21 *Id*.
22 Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).
23 Daniel R. Stoller, *Data Breach Harm Standard May Head to SCOTUS in '17*, BLOOMBERG L. (Dec. 8, 2016, 12:00 AM), https://www.bloomberglaw.com/document/X84N2BT4000000.
24 Keshia Lipscomb & Petrina McDaniel, *Data Breach Laws on the Books in Every State; Federal Data Breach Law Hangs in the Balance*, SECURITY & PRIVACY BYTES (Apr. 30, 2018), https://www.securityprivacybytes.com/2018/04/data-breach-laws-on-the-books-in-every-state-federal-data-breach-law-hangs-in-the-balance/ [https://perma.cc/MU9Q-5JSZ].
25 Kalia & Cohn, *supra* note 16.

information and understand the accompanying anxieties of innocent data breach victims who are put at risk of grave future harm.

As to individual state action, states have imposed their own data security requirements on entities that collect and store consumers' personal information.[26] Many states have passed these laws in the interest of protecting consumers, but each of the fifty-one U.S. data breach protection laws has different standards and requirements, with varying levels of protection for users.[27] While many states have proven capable of developing consumer-friendly statutes, that does not mean that *every* state has, or even that they will. The differences in state laws are worrisome because the amount of protection consumers receive before and after a breach is often determined by where they reside. One example of this is Uber's 2016 breach, where the personal information of roughly 57 million users was compromised.[28] Uber hid the breach from consumers for over a year, "and even used its vulnerability disclosure program to pay the attackers' ransom."[29] In response, many, but not all, states began investigating Uber.[30] Given the scope of Uber's breach, like so many other recent breaches, "a federal standard and a federal investigation would have served [consumers] better—addressing all affected persons in the U.S., not only those living in the states that are investigating the breach."[31]

Two consequences of the unresolved split in federal precedent and the fifty-one different state laws currently in play are of particular concern. First, hundreds of millions of consumers who face the risk of real harm and the resulting practical fears about the misuse of their data are too often barred from court for lack of standing, among other reasons,

---

[26] Monique C.M. Leahy, *Litigation of Data Breach* (2015), *in* 140 AM. JURIS. TRIALS 327, § 3, Westlaw (database updated Oct. 2019) ("Some statutes on data security require businesses to act reasonably to ensure that consumer information is maintained safely within their custody and not susceptible to breach. Other statutes govern specific aspects of data collection and use. Most states have statutes that require consumer notification of a data breach. Some states have statutes governing specific industry data security. Many states do not yet have statutes directly governing general data security practices. Other laws regulating the collection and treatment of particularly sensitive information like Social Security numbers are used instead. State statutes often govern specific industries." (internal footnotes omitted)).

[27] *Security Breach Notification Chart*, PERKINS COIE, https://www.perkinscoie.com/images/content/2/2/v4/220987/Security-Breach-Notification-Law-Chart-June-2019.pdf [https://perma.cc/ZX8A-4VCV] (last modified June 2019); *see* Leahy, *supra* note 26, at § 4 (explaining that states are not in agreement on many important factors concerning breach notification, including what constitutes sensitive personal information, the degree of investigation required post-breach, whom the entities must notify, and the proper form of notification).

[28] Drew Mitnick, *No more waiting: it's time for a federal data breach law in the U.S.*, ACCESS NOW (Apr. 10, 2018, 10:51 AM), https://www.accessnow.org/no-more-waiting-its-time-for-a-federal-data-breach-law-in-the-u-s/ [https://perma.cc/EA8T-CZDA].

[29] *Id*.

[30] *Id*.

[31] *Id*.

and are thus unable to seek redress.[32] Second, the lack of legal accountability means that the entities housing consumers' sensitive information remain disincentivized to take due care and implement security measures to protect them from the next breach.[33] Lowering the standing threshold for data breach victims would impose a much higher cost on companies who do not take adequate steps to protect consumers' data.[34] If increasing liability merely incentivizes entities to fix known security issues or rethink their approach to securing user data, that in and of itself would protect countless consumers.[35] For these reasons, this Note argues that there exists an urgent need for Congress to intervene in this continuing—and growing—problem.

To address the standing issue, a federal statute should clearly define what constitutes an injury in actions brought by data breach victims. Specifically, this Note proposes that Congress imitate California's decision to statutorily define "breach" as inclusive of both the proven tangible misuse of *and* the unauthorized access to consumers' personally identifying information. The California Consumer Privacy Act of 2018 (hereinafter the "California Act" or the "Act")[36] substantially lowers, if not eliminates entirely, the standing hurdle to suits brought by data breach victims.[37] Congress should similarly enact a law that grants a private right of action to any consumer whose non-encrypted or non-redacted personal information has been subject to unauthorized access or misuse as a result of a business's failure to implement and maintain reasonable security procedures. This is the type of protective measure, which has been implemented at the state level in some states, that should be codified in a federal data breach law to ensure uniform protection for consumers.[38]

In order to effectively address the two aforementioned concerns, Congress must enact a federal statute incorporating this facet of the California Act. The statute would resolve the circuit split as to what qualifies as an injury in the data breach context, because the mere breach

---

32 Kalia & Cohn, *supra* note 16.

33 *Id*.

34 *Id*.

35 *Id*.

36 CAL. CIV. CODE § 1798.150 (West 2019) (effective Jan. 1, 2020).

37 Joseph J. Lazzarotti et al., *California May Lower the Standing Threshold in Data Breach Litigation*, JACKSON LEWIS: WORKPLACE PRIVACY, DATA MGMT. & SECURITY REP. (July 11, 2018), https://www.workplaceprivacyreport.com/2018/07/articles/consumer-privacy/california-may-lower-the-standing-threshold-in-data-breach-litigation/ [https://perma.cc/8GHR-C58L].

38 *See* Mitnick, *supra* note 28 (explaining that ideally, a federal statute should both ensure standing and allow states to enact additional protective measures as they see fit); *see also* Lazzarotti et al., *supra* note 37. While "it is crucial that any new federal [data breach] standard does not prevent states from adding protections," there nevertheless remains a need for uniformity at the federal level to set regulations and standards for companies and consumers. Mitnick, *supra* note 28. "A federal breach law should create a floor of minimum standards that companies must meet, not a ceiling prohibiting tougher state enforcement." *Id.*

of a victim's personal information *would be the injury itself*. Such a resolution would ensure that even those plaintiffs whose data has not yet been misused may sue the entities who failed to initially protect it. Allowing such plaintiffs the ability to sue and seek redress is warranted because, outside of data breach cases, courts routinely handle cases where damages are not merely a current financial or property loss.[39] The law has long recognized such intangible harms, including "the infliction of emotional distress, assault, damage to reputation and future business dealings."[40] The law has also long awarded current compensation for potential future pain and suffering, such as to victims of medical malpractice and toxic exposures.[41]

Given the risk and accompanying fear of devastating future harm, data breach victims should not have to prove current, tangible damage *in addition to* the breach of their personal information. "If the fear caused by an assault is actionable, so should the fear caused by the loss of enough personal data for a criminal to take out a mortgage in [the victim's] name."[42] Further, by lowering the standing threshold, more data breach victims would be able to seek redress from the companies that are responsible for the harm they now face. Thus, a federal statute would induce an apprehension of legal accountability.[43] This apprehension would incentivize entities who store and maintain consumer data to implement reasonable security measures to protect against future breaches.[44] This is vital, as consumer data should never fall into the hands of hackers due to a company's negligence in taking steps to protect it.

This Note recommends how a federal law should approach the standing issue in data breach cases and provides support for its conclusion that the mere breach of personal, non-redacted information should be deemed a sufficient injury-in-fact. Part I explains the doctrine of Article III standing, describing its three requirements for a federal lawsuit to qualify as a justiciable case or controversy. Particular attention is drawn to the injury-in-fact prong, as the struggle for data breach plaintiffs often turns on whether the breach of their information *alone* is a sufficient injury. Part II argues that there is an urgent need for Congress to pass a

39 Kalia & Cohn, *supra* note 16.

40 *Id.* ("For harms that can be difficult to quantify, some specific laws[—]e.g.[,] copyright, wiretapping[—]provide for 'statutory damages,' which sets an amount per infraction." (internal footnote omitted)).

41 *Id.*; *see generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422-41 (2013) (Breyer, J., dissenting).

42 Kalia & Cohn, *supra* note 16.

43 *Id*.

44 For a discussion on how companies can protect against data breaches, see Dana Rosenfeld & Donnelly McDowell, *Moving Target: Protecting Against Data Breaches Now and Down the Road*, 28 ANTITRUST 90 (2014).

federal data breach law. It encourages Congress to incorporate components of the California Act into a federal law to achieve a less burdensome standing threshold for data breach plaintiffs. Part II also provides an explanation of how this would incentivize entities that store and maintain consumer data to implement adequate security measures. Part III acknowledges that the private right of action this law would create for those who do not allege misuse may be attacked as running afoul of Article III's case or controversy requirement. To counter that position, Part III discusses precedent that supports the proposed law's constitutionality.

I. ARTICLE III CONSTITUTIONAL STANDING

The U.S. Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies" to ensure that only justiciable cases—those that are appropriate for judicial resolution—are brought before the courts.[45] To bring a federal lawsuit,[46] plaintiffs are required by Article III of the Constitution to establish the "irreducible constitutional minimum of standing."[47] Standing is one of the judicially created doctrines of justiciability and works to define and limit the circumstances under which a federal court may exercise its constitutional authority. According to the Supreme Court, the purpose of Article III standing is to ensure the democratic principle of separation of powers.[48] The standing doctrine places jurisdictional boundaries on the federal courts, thus helping to disable the federal courts from usurping the powers of the other political branches.[49] As explained by the Supreme Court in *Lujan v. Defenders of Wildlife*, whether a plaintiff possesses Article III standing depends on three elements: (1) injury-in-fact suffered by the plaintiff, (2) causation

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

46 Data breach cases, which often take the form of class actions, are generally litigated in federal court. Under the Class Action Fairness Act of 2005 (CAFA), the diversity jurisdiction requirement can be satisfied in a class action lawsuit so long as at least one plaintiff resides in a different state than at least one defendant and the aggregate sum of each individual plaintiff's claim meets or exceeds the $5 million minimum. 28 U.S.C. §§ 1332(d)(2), 1453, 1711-1715 (2012), https://www.congress.gov/109/plaws/publ2/PLAW-109publ2.pdf [https://perma.cc/CFP3-PWPT]; *see generally* Lorio, *supra* note 6, at 82 n.16 ("CAFA has generally been viewed as a tool for limiting class actions because federal courts must apply the strict requirements of Fed. R. Civ. P. 23 as well as consider issues such as Article III standing."); *see also* THOMAS E. WILLGING & SHANNON R. WHEATMAN, AN EMPIRICAL EXAMINATION OF ATTORNEYS' CHOICE OF FORUM IN CLASS ACTION LITIGATION (2005), https://www.uscourts.gov/sites/default/files/clact05.pdf [https://perma.cc/JU4Y-V6JY].

47 *Lujan*, 504 U.S. at 560.

48 Raines v. Byrd, 521 U.S. 811, 820 (1997) (quoting Allen v. Wright, 468 U.S. 737, 752 (1984)) ("[T]he law of Art[icle] III standing is built on a single basic idea—the idea of separation of powers.").

49 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

between the plaintiff's injury and the defendant's conduct, and (3) the likelihood that the injury will be redressed by a favorable decision.[50]

A plaintiff must establish that they have suffered an injury-in-fact before the court can assess the remaining prongs of the standing analysis.[51] Plaintiffs' successful establishment of the requisite injury depends on their ability to show they suffered a violation of a legally protected interest that is "actual or imminent" and "concrete and particularized," as opposed to a type of harm that is merely conjectural or hypothetical.[52] In cases where there is no evidence that the data breach has *already* resulted in misuse of the data, plaintiffs often face a significant hurdle in establishing a sufficient injury.[53] A close analysis of the injury-in-fact prong of the standing doctrine highlights its unique implications in data breach litigation.

A. *Injury-in-Fact: "Actual or Imminent"*

In data breach cases, federal courts have inconsistently ruled on what constitutes an "imminent" injury-in-fact. This split primarily stems from courts' answers to the question of whether a plaintiff, whose personally identifying information was breached by hackers from a defendant company's database but has not yet been fraudulently misused, has suffered a concrete and imminent injury-in-fact. The Supreme Court has repeatedly stated that for an injury to be sufficiently imminent for Article III standing, the injury must be "certainly impending."[54] In *Lujan*, the Court conceded that the imminence requirement is an "elastic concept," but only to the extent that an alleged injury is not too speculative or hypothetical.[55] Thus, the Court indicated that an injury-in-fact may either be present or threatened, so long as it is not too remote or attenuated.[56] A threat does not qualify as a sufficient injury-in-fact when a plaintiff merely alleges an injury at an unspecified future time, and

[50] *Lujan*, 504 U.S. at 560-61 ("First, the plaintiff must have suffered an 'injury in fact'— an invasion of a legally protected interest which is (a) concrete and particularized, and (b) 'actual or imminent, not 'conjectural' or 'hypothetical.' Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.' Third, it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" (internal citations omitted)).

[51] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (quoting Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 103 (1998)) (stating that injury-in-fact is the "'[f]irst and foremost' of standing's three elements").

[52] *Lujan*, 504 U.S. at 560-61.

[53] Kim Phan, *Assessing risk: Data breach litigation in U.S. courts*, IAPP (Nov. 1, 2012), https://iapp.org/news/a/2012-11-01-assessing-risk-data-breach-litigation-in-u-s-courts/ [https://perma.cc/E3PG-UYCU].

[54] *Lujan*, 504 U.S. at 564 n.2.

[55] *Id.*

[56] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

when the resulting harm is "at least partly within the plaintiff's own control."[57] The Court's justification for requiring that an injury possess a "high degree of immediacy" is that it lessens the chance that courts will decide cases where no injury will ever come to fruition.[58]

In 2013, the Court issued a decision on standing in *Clapper v. Amnesty International*,[59] its most recent discussion of the matter. In *Clapper*, the plaintiffs argued that section 702 of the Foreign Intelligence Surveillance Act (FISA) was unconstitutional.[60] Section 702 permits the U.S. government, with the approval of the Foreign Intelligence Surveillance Court (FISA Court), to surveil persons outside of the United States. The plaintiffs were parties who claimed to regularly communicate with individuals living abroad who were accused by the U.S. government of involvement in terrorist organizations.[61] The plaintiffs alleged that FISA would force them to take costly steps to secure communications and evade electronic surveillance, which would injure them financially.[62] The plaintiffs sought to establish injury-in-fact by claiming there was an "objectively reasonable likelihood" that their communications with the individuals living abroad would be intercepted in the future.[63]

The Court rejected the *Clapper* plaintiffs' alleged injury as inconsistent with the requirement that a threatened injury be certainly impending.[64] The alleged financial loss was found too attenuated to be imminent, as it relied on a theory comprised of a "speculative chain of possibilities."[65] The plaintiffs had no actual knowledge of the government's specific targeting of their communications,[66] could not

57 *Lujan*, 504 U.S. at 564 n.2.
58 *Id.*
59 *Clapper*, 568 U.S 398.
60 *Id*. at 407.
61 *Id.* at 406.
62 *Id.* at 406-07 ("Respondents claim that [FISA] compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients. Respondents also assert that they 'have ceased engaging' in certain telephone and e-mail conversations. According to respondents, the threat of surveillance will compel them to travel abroad in order to have in-person conversations. In addition, respondents declare that they have undertaken 'costly and burdensome measures' to protect the confidentiality of sensitive communications." (internal citations omitted)).
63 *Id.* at 410.
64 *Id.*
65 *Id*. (explaining that the plaintiffs' argument relied on a highly speculative and uncertain chain of events that must occur for an injury to materialize: "(1) [T]he Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) the Article III judges who serve on the [Foreign Intelligence Surveillance Court] will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts").
66 *Id.*

prove beyond mere speculation that the government would use section 702 to surveil their communications,[67] and could only speculate that the FISA Court would approve such surveillance if section 702 was chosen, from among many others, as the intelligence-gathering medium.[68] Further, the Court did not think the alleged burden of taking costly steps to secure communications qualified as a present injury. The Court explained that plaintiffs cannot manufacture standing by inflicting harm on themselves based on their fear of hypothetical future harms.[69] To hold otherwise would permit "an enterprising plaintiff [] to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."[70]

Post *Clapper*, it is clear that the injury-in-fact prong will only be satisfied if a plaintiff either alleges a present injury that has already been suffered or a threatened injury in which there is a substantial and non-speculative risk that the plaintiff will incur this harm in the near future.[71] However, it is notable that *Clapper* involved issues of national security. It therefore may be inferred that a concern for separation of powers influenced the Court's decision to refrain from adjudicating the case on its merits. Nevertheless, in the milieu of data breach litigation, *Clapper*'*s* requirements serve as an obstacle for plaintiffs whose data has been breached but has not yet been misused. However, given the perpetual value that most types of personal information possess,[72] hackers are able to retain this information indefinitely. Data breach victims thus encourage the courts to classify their threat of injury as a "substantial risk" of future harm. In sum, successfully alleging an imminent injury-in-fact has proven to be the biggest hurdle for data breach victims seeking redress from the companies who failed to protect their personal data.

B. *Injury-in-Fact: "Concrete and Particularized"*

In addition to being actual or imminent, the injury alleged must be concrete and particularized to satisfy Article III. In *Lujan*, the Court noted that to qualify as particularized, an injury must affect the plaintiff in a "personal and individual way."[73] The converse of a particularized injury

[67] *Id.* at 412.
[68] *Id.* at 413-14.
[69] *Id.* at 415 ("[Plaintiffs] assert that they are suffering ongoing injuries . . . because the risk of surveillance . . . requires them to take costly and burdensome measures to protect the confidentiality of their communications. [Plaintiffs] claim, for instance, that the threat of surveillance sometimes compels them to avoid certain e-mail and phone conversations, to 'tal[k] in generalities rather than specifics,' or to travel so that they can have in-person conversations." (internal citation omitted)).
[70] *Id.* at 416.
[71] *Id.* at 414 n.5.
[72] Shell, *supra* note 8.
[73] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 n.1 (1992); *see* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

is a generalized grievance, which arises in cases where plaintiffs allege a harm that is not specific to them but instead is generally incurred by all the members of a large class.[74] Federal courts have declined to adjudicate such general claims when alleged by an individual plaintiff for the reason that the plaintiff has not established a personal stake in the outcome of the litigation.[75] The Supreme Court, however, has made clear that the particularization inquiry cannot end once it has been established that the injury is specific to the plaintiff, as "particularization is necessary to establish injury in fact, but it is not sufficient."[76] The injury in fact must *also* be concrete, a requirement that, prior to the Court's 2016 decision in *Spokeo v. Robins*, had gone largely undiscussed.[77]

In *Spokeo v. Robins*, consumer plaintiffs brought a class action lawsuit against Spokeo, a consumer reporting agency that searches numerous databases to gather and disseminate personal information about individuals to its users.[78] Spokeo's users include, among others, hiring employers.[79] The representative plaintiff alleged that Spokeo had violated the Fair Credit Reporting Act (FCRA)[80] by releasing false personal information about individuals, including himself, to Spokeo users.[81] The district court held that the plaintiff lacked Article III standing to sue Spokeo because he did not plead a sufficient injury-in-fact. The Ninth Circuit reversed, holding that the plaintiff sufficiently alleged an actual and particularized injury. The court rested its decision on the plaintiff's allegation that "'Spokeo [had] violated *his* statutory rights,'" and on the fact that the plaintiff's "'personal interests in the handling of his credit information [were] *individualized*.'"[82] However, the Supreme Court found that the Ninth Circuit had failed to consider both aspects of the injury-in-fact prong by omitting a discussion of the independent

[74] *Lujan*, 504 U.S. at 573.

[75] Hollingsworth v. Perry, 570 U.S. 693, 706 (2013) (holding that California citizens did not have Article III standing to appeal a federal district court decision holding Proposition 8, a state constitutional amendment banning same-sex marriage, unconstitutional because the outcome of the case did not personally affect them).

[76] *Spokeo*, 136 S. Ct. at 1548.

[77] Lorio, *supra* note 6, at 87.

[78] *Spokeo*, 136 S. Ct. at 1543.

[79] *Id*.

[80] 15 U.S.C. § 1681 (2012), https://www.govinfo.gov/content/pkg/USCODE-2017-title15/pdf/USCODE-2017-title15-chap41-subchapIII.pdf [https://perma.cc/JXB7-E9RV]; *see Spokeo*, 136 S. Ct. at 1545 ("The [FCRA] requires consumer reporting agencies to 'follow reasonable procedures to assure maximum possible accuracy of' consumer reports and imposes liability on '[a]ny person who willfully fails to comply with any requirement [of the Act] with respect to any' individual." (internal citations omitted)).

[81] *Spokeo*, 136 S. Ct. at 1544. The plaintiff alleged that an unknown third party searched his name on Spokeo's website and that the search produced inaccurate information regarding his age, marital status, education, and finances. *Id.*

[82] *Id.* at 1544 (internal citation omitted).

requirement that an injury be "concrete."[83] The Court indicated that particularization and concreteness are two distinct aspects of the injury-in-fact analysis, and a plaintiff must sufficiently plead both in order to have standing to sue.[84]

In *Spokeo*'s majority opinion, Justice Alito stated that for an injury to qualify as "concrete," it must be "*de facto*," meaning it must "actually exist."[85] The injury must, therefore, be one that is "real," as opposed to abstract, but need not necessarily be "tangible."[86] While often more difficult to recognize, intangible injuries may nevertheless be concrete enough to constitute an injury-in-fact, a determination that rests on "both history and the judgment of Congress."[87] Regarding the latter, the Court reiterated Congress's authority to elevate previously inadequate intangible harms to the level of requisite concreteness necessary for Article III standing.[88] However, the Court made clear that a plaintiff would not "automatically satisf[y] the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[89] In other words, Article III requires the allegation of a concrete injury *despite* the presence of a statutory violation.[90]

The Court held that the procedural violation alleged in *Spokeo*, without an accompanying concrete harm, did not satisfy the injury-in-fact requirement.[91] Because a "bare procedural violation" does not necessarily result in a concrete injury, Spokeo's violation of one FRCA procedural requirement may likely result in no harm to the plaintiff at all.[92] The Court deemed the alleged injury unsatisfactory for Article III standing, despite

83 *Id.*; *see* Robins v. Spokeo, Inc., 742 F.3d 409, 413 (9th Cir. 2014) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 578 (1992)) (conclusively grouping "concreteness" with the "particularized" requirement by stating that "the interests protected by the statutory rights at issue are sufficiently concrete and particularized that Congress can elevate them").

84 *Spokeo*, 136 S. Ct. at 1548.

85 *Id.*

86 *Id.* at 1549 ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." (internal citations omitted)); *see, e.g.*, Pleasant Grove City v. Summum, 555 U.S. 460 (2009) (free speech); *see also* Church of Lukumi Babalu Aye, Inc. v. Hialeah, 508 U.S. 520 (1993) (free exercise).

87 *Spokeo*, 136 S. Ct. at 1549.

88 *Id.* at 1548 (citing *Lujan*, 504 U.S. at 578).

89 *Id.* at 1549.

90 *Id.* (clarifying that the Article III requirement does not suggest that a *risk* of real harm is incapable of being concrete).

91 *Id.*

92 *Id.* at 1550 ("A violation of one of the FCRA's procedural requirements may result in no harm. For example, even if a consumer reporting agency fails to provide the required notice to a user of the agency's consumer information, that information regardless may be entirely accurate. In addition, not all inaccuracies cause harm or present any material risk of harm. An example that comes readily to mind is an incorrect zip code. It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm.").

the fact that Spokeo was legally forbidden from publishing false information about individuals and that the plaintiff had initially brought this suit in direct response to Spokeo's alleged release of false information particularly involving the plaintiff.[93] Furthermore, the Court did not deem the risk of harm that could flow from such an inaccurate representation of one's personal information sufficiently injurious to serve as grounds for a lawsuit under the FCRA.[94]

II. CALIFORNIA'S APPROACH TO DATA BREACH STANDING

Since *Clapper*, and especially since *Spokeo*,[95] a split in precedent has developed regarding whether individuals whose information was compromised[96] by a data breach, without proof of misuse, have suffered a concrete and imminent Article III injury. The inconsistent standards among the federal courts stem from the courts' answers to the question of whether an increased risk of future harm, standing alone, is sufficient to confer standing.[97] After a data breach, affected consumers seek to recover costs from the companies who put them in a harmful position by negligently failing to protect their stored data. For plaintiffs who cannot yet prove misuse of their compromised information, the injury alleged is often an increased risk of future harm. Sometimes, these plaintiffs further allege the injury of financial loss suffered from credit monitoring and fraud prevention service fees was incurred *due to* their risk of future harm. The federal courts handle injury allegations without proof of misuse differently, leaving many plaintiffs unable to sue the companies who failed to protect their personal data.

However, outside of the data breach context, courts routinely handle cases where the injuries alleged are not current, tangible losses, but intangible harms such as assault, damage to reputation and future business dealings, and infliction of emotional distress.[98] Courts have also long awarded current compensation for potential future pain and suffering, for example to victims of medical malpractice and toxic exposures.[99] Further, the U.S. Supreme Court has recognized that there is

93 Michael C. Dorf, *Supreme Court Requires "Concrete" Injury for Standing*, JUSTIA: VERDICT (May 18, 2016), https://verdict.justia.com/2016/05/18/supreme-court-requires-concrete-injury-standing [https://perma.cc/H2GB-H3W2].

94 *Id.*

95 *See* Allison Holt et al., *Standing in the Midst of a Data Breach Class Action*, 84 DEF. COUNS. J. 1, 9 (2017).

96 The term "compromised" in this Note refers to data that was obtained by hackers through their unauthorized access to a company's stored non-encrypted or non-redacted personally identifying consumer information.

97 Stoller, *supra* note 23.

98 Kalia & Cohn, *supra* note 16.

99 *Id.*; *see generally* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422-41 (2013) (Breyer, J., dissenting).

a reasonable probability of future injury for one who is faced with a present situation that requires them to take protective measures to mitigate or prevent the potential effects of the probable future injury.[100] Justice Breyer's dissent in *Clapper* emphasized these points, arguing that courts have often found probabilistic injuries as sufficient to support standing outside of the data breach context. He asserted that, despite the inherent uncertainty of alleged future injuries, such as an anticipatory breach of contract, the Constitution does not prohibit federal courts from hearing such claims.[101] The same principle should apply in data breach litigation. Given the increased role of technology in everyday life, consumers are more frequently storing their personal information in digital mediums, and hackers are getting smarter.[102] It is time data breach plaintiffs are able to seek legal redress for the severe harm they face when their sensitive data is stolen.[103]

Congress should address the standing issue faced by data breach victims and implement a federal statute that clearly defines what constitutes a sufficient Article III injury. This Note proposes that Congress should define injury broadly to encompass not only proven misuse, but also unauthorized access to consumers' sensitive information. Such a broad definition, which classifies the mere breach of one's data as a sufficient injury, would allow data breach victims to at least make it through the courthouse door. Data breach victims should not bear the additional burden of proving actual misuse of sensitive information when a company has already failed to adequately secure it in the first place. The data, which does not lose its value after it has been hacked and remains in hackers' possession for potential future misuse, should not have been susceptible to hacking in the first place. Given the near impossibility of taking part in today's economy without frequently sharing personally identifying information,[104] it must follow that companies that acquire and store this sensitive information should be held accountable for their inadequate security measures.

This Note encourages Congress to imitate the California legislature's enactment of the California Act, which allows consumers to sue a business in response to a data breach without a showing of additional misuse of that data. This statute essentially eliminates the standing issue encountered by many data breach plaintiffs.[105] In his

100 *Clapper*, 568 U.S. at 437-38 (referencing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 152-53 (2010)).
101 *Id.* at 436.
102 *See* Lorio, *supra* note 6; *see also* Weisbaum, *supra* note 12.
103 *See* discussion *supra* Introduction.
104 Lorio, *supra* note 6, at 118.
105 CAL. CIV. CODE § 1798.150 (West 2019) (effective Jan. 1, 2020).

introduction to the California Act, Senator Bill Dodd "stressed the importance of providing consumers a measure to sue following a data breach of their personal information."[106] While many states have adopted protective standards for consumers in the data breach context, California's law is perhaps the most consumer-friendly in terms of enabling court access. This Note stresses the importance of providing standing to all U.S. consumers whose personal information has been compromised. Thus, it is crucial that a federal law imitates California's action of lowering the standing bar instead of waiting on the rest of the states to do so independently. What follows is an account of the relevant provisions of the California Act for purposes of this Note's argument.

In addition to providing for the Act's enforcement by the Attorney General, the California Act creates a private right of action for consumers in the wake of a data breach. This private right of action is limited to cases in which there was a data breach involving consumers' "non-encrypted or non-redacted personal information" due to the company's failure to implement and maintain the reasonable security procedures necessary to protect it.[107] Specifically, beginning January 1, 2020, section 1798.150 of the California Civil Code will serve two important objectives: First, this section will expand the applicability of the cause of action established therein to "[a]ny consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure,"[108] and not just to those allegations asserting misuse or harm beyond a hacker's mere access. Second, this section includes a safe harbor provision that will grant those businesses not in "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the [consumer's] personal information" protection from legal liability.[109] Accordingly, once effective, the enforcement of this statute will be positive for both consumers and entities alike: Not only will it "provide greater protection to consumer's personal information" and "substantially lower . . . the standing threshold in data breach . . . lawsuits,"[110] but it will also incentivize businesses to adequately safeguard all sensitive customer information by affording legal protection to any business that employs sufficient security measures.

Importantly, for purposes of determining what data qualifies as sensitive, section 1798.81.5 of the California Civil Code defines

106 Lazzarotti et al., *supra* note 37.
107 CIV. § 1798.150(a)(1) (effective Jan. 1, 2020).
108 *Id.*
109 *Id.*; *see* Lazzarotti et al., *supra* note 37.
110 Lazzarotti et al., *supra* note 37.

"personal information" broadly.[111] Under the California Act, information is deemed "personal" where it either comprises: "(A) an individual's first name or first initial and his or her last name in combination with one or more . . . data elements"[112]—specifically, "(i) [s]ocial security number[,] (ii) [d]river's license number or California identification card number[,] (iii) [a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial account[,] (iv) [m]edical information[, and/or] (v) [h]ealth insurance information"[113]—"when either the name or the data elements are not encrypted or redacted;" or "(B) a username or email address in combination with a password or security question and answer that would permit access to an online account."[114] Explicitly excluded from the Act's definition of "personal information" is any consumer information that is made available to the general public in a lawful manner through federal, state, or local government records.[115] This fact overcomes the argument that lowering the standing threshold in data breach cases would incite frivolous lawsuits, as it limits the type of data for which consumers may seek legal redress.[116]

Under the California Act, a consumer may initiate "a civil action for any of the following: (A) [t]o recover damages in an amount not less than . . . $100 . . . and not greater than . . . $750[;] . . . . (B) [i]njunctive or declaratory relief[; and/or] (C) [a]ny other relief the court deems proper."[117] Moreover, under the directive of the Act, California courts are

111 *Id*.

112 CIV. § 1798.81.5(d)(1)(A).

113 *Id.* § 1798.81.5(d)(1)(A)(i)-(v); *see id.* § 1798.81.5(d)(2) ("'Medical information' means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional."); *see also id.* § 1798.81.5(d)(3) ("'Health insurance information' means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.").

114 *Id.* § 1798.81.5(d)(1)(A)-(B).

115 *Id.* § 1798.81.5(d)(4) ("'Personal information' does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.").

116 Kristen L. Burge, *Your Data Was Stolen, But Not Your Identity (Yet)*, ABA (Jan. 11, 2018), https://www.americanbar.org/groups/litigation/publications/litigation-news/featured-articles/2018/your-data-was-stolen-not-your-identity-yet/ [https://perma.cc/T955-4RF6] ("The question of the threat or imminence of injury from a security incident should turn on the type of data that was compromised . . . . For instance, when stolen data are sensitive information that can readily be exploited for gain, like financial account numbers and credentials, login credentials and passwords to e-commerce sites or email accounts, Social Security numbers, drivers' license numbers, and similar information, the likelihood that the information is going to be misused is high . . . . But the same cannot be said for information that is generally available, like names, birthdates, and email addresses (without login credentials) . . . . If data can be accessed publicly, such as a person's email address, home address, telephone number, or birth date, how does the compromise of that information cause a certainly impending injury?").

117 CIV. § 1798.150(a)(1)(A)-(C) (effective Jan. 1, 2020).

afforded considerable guidance in assessing the appropriate amount of statutory damages to be rewarded in a given case.[118] Specifically, the courts are directed to consider "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."[119] Additionally, pursuant to the requirements stipulated in section 1798.150(b), a consumer, before "initiating any action against a business for statutory damages[,] . . . [must] "provide[] a business [thirty] days' written notice identifying the specific provisions of [the California Consumer Privacy Act] the consumer alleges have been . . . violated."[120] However, "if within the [thirty] days the business . . . cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for . . . statutory damages . . . may be initiated against the business."[121]

The notice provision, once implemented, will likely encourage entities to be diligent in their efforts to try to cure alleged issues to avoid legal action.[122] This will arguably incentivize entities to preemptively adopt cybersecurity measures that are capable of remedying anticipated issues in a timely fashion.[123] Considering the exponentially growing risk of legal liability as a result of data breaches, companies will be more inclined to ensure that they have comprehensive data protection and incident response plans in place should such an incident arise[124]—and that such plans take into consideration factors like the type of data stored, the storage mechanisms, and the duration of storage.[125] Given the current patchwork of state laws governing data security that companies must comply with, this task remains considerably difficult.[126] By establishing a national standard for data security, Congress would facilitate compliance with data security laws for entities that acquire and maintain consumer information, as it would rid them of the burden of monitoring the maze of state data breach laws that currently exists.[127]

118 *Id.* § 1798.150(a)(2) (effective Jan. 1, 2020).
119 *Id.*
120 *Id.* § 1798.150(b) (effective Jan. 1, 2020).
121 *Id.*
122 Stephen Lilley et al., *New California Consumer Privacy Act increases the risk of additional data breach class actions*, MAYER BROWN: CLASS DEF. BLOG (July 19, 2018), https://www.classdefenseblog.com/2018/07/new-california-consumer-privacy-act-increases-risk-additional-data-breach-class-actions/ [https://perma.cc/AP9J-DL45].
123 *Id*.
124 Rosenfeld & McDowell, *supra* note 44.
125 *Id*.
126 *See* Mitnick, *supra* note 28.
127 *Id.*

III. CURRENT CASE LAW: THE PROPOSED CONGRESSIONAL AUTHORIZATION OF A PRIVATE RIGHT OF ACTION TO DATA BREACH PLAINTIFFS DOES NOT VIOLATE ARTICLE III'S "CASE OR CONTROVERSY" REQUIREMENT

This Note anticipates the primary argument in opposition to the adoption of the federal statute for which it advocates: that the private right of action it would confer on plaintiffs who have not yet suffered misuse runs afoul of Article III's case or controversy requirement. However, the proposed statute is supported by the precedent of numerous federal circuit courts, which deem the proposed statute's definition of "injury" for a private right of action satisfactory for Article III standing. This Note will thus proceed with a reiteration of the scope of Congress' power to statutorily create legal rights for plaintiffs, as well as a discussion of the arguments likely to be made against a finding of standing when the injury alleged is merely an increased risk of future harm. This Note will then provide case law that supports a federal statute's conferral of a private right of action to prove that such a statute would satisfy Article III's case or controversy requirement.

As was previously mentioned, *Spokeo* conveyed the important point that while Congress may statutorily deem injuries legally cognizable, it is prohibited from giving individuals a free pass to exercise a statutory right to sue merely because that right is codified in the law.[128] Specifically, Article III requires the presence of a concrete injury notwithstanding a given statute's creation of a private right of action.[129] This principle is reflected in the *Lujan* majority's discussion of the Endangered Species Act (ESA), which created a private right of action for the plaintiffs to initiate suit upon the statute's violation.[130] The Court concluded that, although the plaintiffs had satisfied the ESA requirements necessary to invoke a statutory right of action, they nonetheless failed to establish an injury-in-fact with the requisite imminence to establish Article III standing.[131] The Court emphasized that, for purposes of Article III standing, a plaintiff's injury must be concrete and particularized, and criticized statutes like the ESA, which created a federal cause of action

128 Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016); *see* Lorio, *supra* note 6, at 114-15; *see also* discussion *supra* Part I.B.

129 *Spokeo*, 136 S. Ct. at 1549; *see* Lorio, *supra* note 6, at 115 ("Any law that purports to create a private right of action that bypasses Article III standing requirements is unconstitutional." (internal footnote omitted)); *see* John G. Roberts, Jr., *Article III Limits on Statutory Standing*, 42 DUKE L.J. 1219, 1226-29 (1993), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3224&context=dlj [https://perma.cc/2Z5V-CTRP]; *see also* discussion *supra* Part I.B.

130 Lujan v. Defs. of Wildlife, 504 U.S. 555, 558 (1992).

131 *Id.* at 564, 566-67 ("Such 'some day' intentions—without any description of concrete plans, or indeed even any specification of *when* the some day will be—do not support a finding of the 'actual or imminent' injury that our cases require.").

for a harm generally suffered by all citizens or all members of a large class of citizens.[132]

However, while the *Lujan* Court held such generalized grievance statutes to be unconstitutional, it recognized that an Article III injury might nevertheless exist on the sole ground that a statutorily created legal right was invaded.[133] While Congress does have the power to confer private rights of action statutorily, that power does not go unchecked. *Lujan* makes clear that Congress is limited in this respect; a federal statute that is too broad or general will be challenged as violating Article III's requirement that only justiciable cases or controversies be adjudicated. Thus, while an Article III injury may exist solely by virtue of an invasion of a statutorily created right, the federal statute proposed herein—which would create a private right of action for individuals whose data has not yet been misused—would likely be met with concerns similar to those raised in *Lujan*.

Those who favor a narrow standing analysis would likely challenge the proposed statute as an abuse of congressional power for granting data breach victims a "blank check" to sue. Opponents would almost certainly argue that the proposed statute is too broad—and, therefore, any violation of it could not be considered "concrete and particular" to the individual consumers under the standard established in *Lujan*. Moreover, following *Lujan*, opponents may attack the injury alleged in such a statutorily permitted action as being neither actual nor imminent. Such criticism would specifically target consumers who allege a risk of harm in the wake of a breach, but who do not have proof of misuse. That category of consumers could be particularly vulnerable to the argument that the mere breach of their data is not sufficiently imminent to pass constitutional muster. These arguments are anticipated based on the case law of the Third, Fourth, and Eighth Circuits—three federal circuit courts that have repeatedly shut their doors to plaintiffs who failed to allege a tangible injury regarding the breach of their personal information.

In the context of data breach claims where the misuse of one's personal information cannot yet be proven, the injury allegations set forth often include: (1) an increased risk of substantial future harm that the consumer now faces, and/or (2) a financial loss incurred by the consumer in an effort to prevent or mitigate the risk of future misuse.[134] Proponents

132 *Id.* at 573-74; *see also* discussion *supra* Part I.B.

133 *Lujan*, 504 U.S. at 578 (quoting Warth v. Seldin, 422 U.S. 490, 500 (1975)) ("[T]he . . . injury required by Art[icle] III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'").

134 Catherine Padhi, *Standing in Data-Breach Actions: Injury in Fact?*, LAWFARE (Dec. 18, 2017, 7:00 AM), https://www.lawfareblog.com/standing-data-breach-actions-injury-fact [https://perma.cc/GWE9-4SSU] (stating that a theory of harm for data breach plaintiffs is that of a substantial risk of future harm); *see* Lorio, *supra* note 6, at 93 (noting Lewert v. P.F. Chang's China

of a narrow approach to standing—specifically the Third, Fourth, and Eighth Circuits—think it is too *speculative* and *conjectural* to consider the alleged risk of future harm due to the mere breach of the sensitive data as an Article III injury.[135] These proponents reason that such damage would flow, *if at all*, from an injury that has not yet occurred.[136] In essence, these courts use a strict interpretation of the injury-in-fact requirement to limit the data breach cases litigated in federal court to those in which the plaintiff alleges a tangible misuse of their personal information.[137]

Moreover, relying heavily on the Supreme Court's ruling in *Clapper*, these courts deem the likelihood of future injury to any single person whose information was seen or obtained by hackers in a data breach to be too attenuated to qualify as imminent.[138] These courts generally require plaintiffs to make some showing that their personal information is being used in a way that harms them—i.e., through identity theft or fraud.[139] These courts also hold that, although commonly alleged, financial loss incurred from the cost of preventative measures taken in response to a breach cannot be considered an "actual" injury.[140] In support of the position that this kind of financial loss cannot satisfy Article III's injury requirement, courts reason that the plaintiffs willingly incurred such costs to protect against hypothetical future events.[141]

Bistro, Inc., 819 F.3d 963 (7th Cir. 2019)) (stating that "both plaintiffs [in *Lewert*] asserted that they were injured because they spent time and money monitoring their credit").

135 Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011), *cert. denied*, 566 U.S. 989 (2012); *see* Beck v. McDonald, 848 F.3d 262, 267 (4th Cir. 2017), *cert. denied*, 137 S. Ct. 2307 (2017); *see also In re* SuperValu, Inc., Customer Data Sec. Breach Litig., 870 F.3d 763, 771-72 (8th Cir. 2017), *aff'd*, 925 F.3d 955 (8th Cir. 2019).

136 *See* cases cited *supra* note 135.

137 James Giszczak et al., *Risk of future identity theft may be sufficient to confer standing in data breach litigation*, MCDONALD HOPKINS: BUS. ADVOC. (Mar. 06, 2018), https://mcdonaldhopkins.com/Insights/Blog/Data-Privacy-Solutions/2018/03/06/Risk-of-future-identity-theft-may-be-sufficient-to-confer-standing-in-data-breach-litigation [https://perma.cc/9WN8-5V4N].

138 *See* Burge, *supra* note 116.

139 *Reilly*, 664 F.3d at 46.

140 *Id.* ("That a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a 'concrete and particularized' or 'actual or imminent' injury." (internal citation omitted)); *see generally Beck*, 848 F.3d 262 (holding that, because a plaintiff may not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending," the plaintiffs failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing); *see also In re SuperValu, Inc.*, *Customer Data Sec. Breach Litig.*, 870 F.3d at 771-72 ("Because [the] plaintiffs [did] not allege[] a substantial risk of future identity theft, the time they spent protecting themselves against th[at] speculative threat [could not] create an injury. Accordingly, . . . [since] the complaint [did] not sufficiently allege[] a substantial risk of identity theft, . . . [the] plaintiffs' allegations of future injury d[id] not [confer Article III] standing. . . ." (internal citations omitted)).

141 *See* cases cited *supra* note 140.

A. *Case Law in Support of the Proposed Federal Statute*

Despite the contrary precedent created by the Third, Fourth, and Eighth Circuits, there is ample support for this Note's proposed federal statute in the case law of the Sixth, Seventh, Ninth, Eleventh, and District of Columbia Circuits. In these circuits, data breach plaintiffs who did not allege that misuse occurred have categorically succeeded in persuading the courts that their injury was sufficient to confer Article III standing.[142] The courts that have maintained this more liberal approach to standing in data breach lawsuits have consistently reduced the burden on plaintiffs to bring a prima facie claim, thereby allowing them, at the very least, to withstand motions to dismiss. Moreover, these courts have adopted the most lenient standards of Article III standing in the data breach context, permitting data breach victims to seek legal recourse merely because their personal information was exposed to hackers.[143] A federal data breach statute should recognize and incorporate what these courts have consistently deemed to be imminent, concrete, and particularized injuries appropriate for adjudication. Therefore, the federal statute proposed by this Note follows the precedent of those courts, which have repeatedly held that, even in the absence of misuse, the injury allegations of data breach plaintiffs may nevertheless be both concrete and particularized, as well as actual or imminent, to satisfy the Article III case or controversy requirement.

B. *Concrete and Particularized*

In *Lujan*, the Court held that because the ESA's statutory right of action to sue the U.S. government for its violation was granted to "any person," it was too broad to meet the requisite particularization threshold.[144] However, a federal data breach statute could be written narrowly to avoid inadequacy under the standing analysis by restricting the class of plaintiffs with the right to sue to only those consumers whose personal information was accessed in a given breach. By adopting the California Act's limited extension of the right to sue to only those whose "nonencrypted or nonredacted personal information" was accessed and thereby excluding from protection any information made legally available to the general public, Congress could ensure that the scope of the proposed federal statute has a narrow application.[145] Therefore, in the

142 Lorio, *supra* note 6, at 100.
143 *Id.* at 91.
144 *Id.* at 116 (citing 16 U.S.C. § 1540(g) (2012), https://www.govinfo.gov/content/pkg/ USCODE-2002-title16/pdf/USCODE-2002-title16-chap35-sec1540.pdf [https://perma.cc/3SDQ-T7GA]).
145 CAL. CIV. CODE § 1798.150(a)(1) (West 2019) (effective Jan. 1, 2020).

event of a data breach, only those defendant companies that did not adequately protect their customers' information could be held liable.[146]

In *Attias v. CareFirst*, the court stated that "nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury," suggesting that the D.C. Circuit takes for granted the existence of concreteness and particularization in data breach cases.[147] This unequivocal approach to those standing elements can be attributed to the fact that the fraudulent use or theft of a consumer's personal information, or an imminent risk thereof, undoubtedly constitutes a concrete and particularized injury. If this is true, and the fraudulent use or theft of a consumer's personal information does indeed constitute a concrete and particularized injury, then the only remaining question for courts is whether the complaint plausibly alleges that, although no misuse has occurred, the plaintiff is now at a substantial risk of misuse as a result of the company's failure to protect their information.[148] Following this line of reasoning, the *Spokeo* court's determination that a "bare procedural violation" cannot constitute an injury-in-fact would not be implicated in the passage of the proposed federal data breach law. In other words, although plaintiffs would be suing pursuant to a statutorily created right, because the alleged injury would already be characterized as concrete and particularized, the courts would be left to determine only whether the injury was actual or imminent enough to establish Article III standing.

C. *Actual or Imminent*

Several plaintiff-friendly courts have held that, in the absence of misuse, an alleged increased risk of substantial future harm and/or financial loss incurred from precautions taken to prevent or mitigate the risk of misuse are both sufficient Article III injuries.[149] Specifically, these courts have consistently held that the threat to plaintiffs whose information was compromised in a data breach is certainly impending because it is highly likely that they will fall victim to identity theft or fraud.[150]

146 Lorio, *supra* note 6, at 119.
147 Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017).
148 *Id.*
149 Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); *see* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); *see also* Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010); *see also In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).
150 Burge, *supra* note 116.

D. *The Sixth Circuit*

Shortly after *Spokeo* was decided, the Sixth Circuit delivered its opinion on what constitutes sufficient injury for Article III standing in data breach cases in *Galaria v. Nationwide Mutual Insurance*.[151] In *Galaria*, Nationwide, an insurance and financial services company, maintained records that contained its customers' personal information, including names, dates of birth, marital statuses, genders, occupations, employers, social security numbers, and driver's license numbers.[152] In 2012, a group of hackers gained acces to Nationwide's computer network, which contained the personal information of 1.1 million Nationwide customers—including the two plaintiffs in *Galaria*.[153] The customers whose information was hacked filed a class action lawsuit against Nationwide, alleging that the breach created an "imminent, immediate and continuing increased risk" that they would be subject to identity fraud.[154] The plaintiffs therefore sought damages for the increased risk of fraud, the expenses incurred to mitigate that risk, and the time spent on such mitigation efforts.[155]

The court ultimately held that the *Galaria* plaintiffs' allegations of a substantial risk of harm, in addition to their reasonably incurred mitigation costs, were sufficient to establish a legally cognizable Article III injury.[156] The court acknowledged that, unlike the injuries deemed insufficient in *Clapper*, the *Galaria* plaintiffs' had alleged injuries that were not merely speculative claims of a "possible future injury" or an "objectively reasonable likelihood."[157] The court stated that it was unnecessary to speculate in cases "where [the] Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."[158] Instead, where a data breach targets personal information, it can be reasonably inferred that the hacker will use that information for the fraudulent purposes alleged in the plaintiffs' complaint.[159]

After finding that there was a substantial risk of harm to the *Galaria* plaintiffs, the court concluded that it was reasonable for the plaintiffs to

151 *Galaria*, 663 F. App'x 384.
152 *Id.* at 386.
153 *Id.*
154 *Id.* ("In support of their claims, Plaintiffs allege that there is an illicit international market for stolen data, which is used to obtain identification, government benefits, employment, housing, medical services, financial services, and credit and debit cards. Identity thieves may also use a victim's identity when arrested, resulting in warrants issued in the victim's name.").
155 *Id.*
156 *Id.* at 388-90 (explaining that "the intentional theft of [plaintiffs'] data" constituted an "identifiable taking").
157 Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408-11 (2013).
158 *Galaria*, 663 F. App'x at 388.
159 *Id.*

take the protective measures that led them to incur mitigation costs.[160] Even in the absence of certainty that the plaintiffs' data would be misused, the court was comfortable reaching this conclusion because the plaintiffs already knew that they no longer unilaterally controlled their data.[161] Thus, the court thought it would be unreasonable to expect the plaintiffs to wait for actual misuse to occur before taking steps to ensure their personal and financial security.[162] On this point, the court found it noteworthy that Nationwide had encouraged the plaintiffs to take steps to mitigate their increased risk of harm and had even offered credit-monitoring and identity theft protection for one year post-breach.[163]

E. *The Seventh Circuit*

In two cases following *Clapper*, the Seventh Circuit has recognized that, under certain circumstances, a "substantial risk" will suffice to establish Article III standing in a data breach action. In *Remijas v. Neiman Marcus Group, LLC*, the plaintiffs brought a class action lawsuit against Neiman Marcus Group, LLC, after approximately 350,000 Neiman Marcus customers' payment card information was compromised in a cyberattack on the department store's database.[164] Notably, of the 350,000 cards that were potentially exposed in the data breach, only 9,200 had been used fraudulently.[165] The plaintiffs specifically alleged that they possessed standing to sue based on several injuries, including: (1) increased risk of future fraudulent charges, and (2) a greater susceptibility to identity theft.[166] The question presented to the Seventh Circuit was whether those allegations satisfied *Clapper's* requirement that an alleged future injury be "certainly impending."[167]

The *Remijas* court held that the injuries raised by the plaintiffs were not mere allegations of possible future injury, but instead were the type of "certainly impending" future injuries that the Supreme Court required to confer standing.[168] In distinguishing this case from *Clapper*, the

160 *Id.*
161 *Id.*
162 *Id.*
163 *Id.* at 386 ("Nationwide informed Plaintiffs of the breach in a letter that advised taking steps to prevent or mitigate misuse of the stolen data, including monitoring bank statements and credit reports for unusual activity. To that end, Nationwide offered a year of free credit monitoring and identity-fraud protection of up to $1 million through a third-party vendor. Nationwide also suggested that Plaintiffs set up a fraud alert and place a security freeze on their credit reports. However, Nationwide's website explained that a security freeze could impede consumers' ability to obtain credit, and could cost a fee between $5 and $20 to both place and remove. Nationwide did not offer to pay for expenses associated with a security freeze.").
164 Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 689-90 (7th Cir. 2015).
165 *Id.* at 690.
166 *Id.* at 692.
167 *Id*.
168 *Id.* at 693-94.

Seventh Circuit held that the plaintiffs' claims did not rest on a highly speculative or attenuated chain of events because the risk that their personal information would be misused was both "immediate and very real."[169] Moreover, the court determined that it was reasonable to presume that the hacker's purpose for infiltrating the store's database and stealing its customers' sensitive information was to eventually use that information to make fraudulent charges or engage in identity theft.[170] The court thus found no reason to speculate as to whether the Neiman Marcus customers' data had been stolen, nor to hypothesize about the nature of the information obtained—given the objectively reasonable likelihood that future misuse would occur, the court saw no reason to force the plaintiffs to wait until their data was fraudulently used to confer standing.[171]

In making this determination, the court gave serious consideration to the Government Accountability Office Report cited by the plaintiffs, which stated that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data ha[s] been sold or posted on the Web, fraudulent use of that information may continue for years."[172] Based on these findings, the court held that it was reasonable to infer that the plaintiffs sufficiently stated a substantial risk of harm due to the data breach. The court emphasized that while the plaintiffs might ultimately fail to present a sufficient factual basis to support this inference at a later point, they had no such burden at the pleading stage and therefore should not be deprived of standing.[173]

With respect to the plaintiffs' allegation of financial loss incurred from the costs of their efforts to protect against future misuse of their data, the Seventh Circuit concluded that mitigation expenses qualify as actual injuries where harm is imminent.[174] Once again distinguishing the present case from *Clapper*, the *Remijas* court emphasized that this case did not fall within the category of cases addressing "speculative harm based on something that may not even have happened to some or all of the plaintiffs."[175] Importantly, Neiman Marcus did not contest the fact that the initial breach took place; in fact, it even offered complimentary credit monitoring and identity theft protection services for one year to all of its customers whose personal information was stored on its database,

169 *Id.* at 693 (citing *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014)).
170 *Id.*
171 *Id.*
172 *Id.* at 694.
173 *Id.*
174 *Id.*; *see* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) ("In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid the harm." (internal citation omitted)).
175 *Remijas*, 794 F.3d at 694.

as well as to any customers who had shopped at one of the store's locations, during the timeframe relevant to the breach.[176] Based on this information, the court found it reasonable that an affected customer might find it necessary to obtain further mitigation services to protect against any future misuse of their personal information.[177]

The Seventh Circuit once again reiterated its broad approach to standing in cases concerning allegations of a data breach in *Lewert v. P.F. Chang's China Bistro, Inc*.[178] In *Lewert*, the restaurant chain P.F. Chang's suffered a data breach in which hackers stole its consumers' credit and debit card information.[179] At the time of the breach, P.F. Chang's did not know the number of consumers or which of its specific locations was affected by the breach.[180] Given this uncertainty, P.F. Chang's implemented nationwide precautionary measures, directing all of its locations to switch to a manual card-processing system and recommending that every customer monitor their credit and/or debit card statements.[181] Despite its adoption of such broad precautionary measures, P.F. Chang's ultimately discovered that only thirty-three restaurants were affected by the data breach.[182] Two customers who had dined at one of P.F. Chang's affected restaurants months before the breach brought a class action suit on behalf of all the customers whose card payment information might have been compromised in the breach.[183]

Notably, of the two named plaintiffs, only one experienced fraudulent transactions with the card he had used at P.F. Chang's[184]—and he canceled his card and purchased a credit monitoring service promptly upon discovering the fraudulent transactions.[185] While the other plaintiff did not experience any fraudulent transactions, he nonetheless alleged that he had spent time and effort monitoring his card statements and credit report to ensure that no fraudulent charges were made and no fraudulent accounts were opened in his name as a result of the breach.[186] Given the fact that their data had already been stolen, the plaintiffs alleged increased risk of fraudulent charges and identity theft.[187]

Finding that the alleged future injuries were sufficient to support Article III standing, the court reaffirmed its contention that a substantial

176 *Id.*
177 *Id.*
178 Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016).
179 *Id.* at 965.
180 *Id.*
181 *Id.*
182 *Id.*
183 *Id.*
184 *Id.*
185 *Id.*
186 *Id.*
187 *Id.* at 967.

risk of harm can be inferred in the wake of a data breach—based on the hacker's undeniable goal of eventually making fraudulent use of consumers' data.[188] Moreover, the court reemphasized that the time and money that the plaintiffs had spent resolving the fraudulent charges established a legally cognizable injury for purposes of establishing Article III standing; it therefore found that the plaintiffs alleged sufficient facts regarding their present injuries to support standing.[189] Specifically, one plaintiff alleged that, although the bank stopped the fraudulent charges on his card before they were processed, he was nevertheless injured by the time and effort he spent resolving the fraud, as well as by the costs incurred from purchasing a credit monitoring service to mitigate his risk.[190] Similarly, the other plaintiff alleged that the time and effort he spent monitoring his financial information to mitigate the risk of future misuse likewise constituted an injury.[191]

In an attempt to distinguish the present case from *Remijas*, P.F. Chang's argued that, unlike Neiman Marcus, it did contest whether its consumers' data was compromised in the breach.[192] However, the court held that at the pleading stage of litigation the plaintiffs' factual allegations to support standing need only be plausible, so it was irrelevant whether or not P.F. Chang's could assert a valid distinction between the current case and *Remijas*.[193] The court concluded that the plaintiffs' allegations were plausible because P.F. Chang's did not initially know how many or which of its stores were affected by the breach, and it reacted as though the breach had affected all of its locations.[194] Therefore, the court found that it was reasonable for the plaintiffs to presume that P.F. Chang's thought the risk was high enough to suggest that all customers engage in credit monitoring and that all its locations switch to manual card-processing.[195]

F. *The Ninth Circuit*

In 2010, the Ninth Circuit decided *Krottner v. Starbucks Corp.*, a case concerning a stolen laptop containing the unencrypted names, addresses, and social security numbers of roughly 97,000 Starbucks

188 *Id.*
189 *Id.*
190 *Id.*
191 *Id.*
192 *Id.* at 967-68.
193 *Id.* at 968; *see* Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007); *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992) (holding that each element of standing "must be supported . . . with the manner and degree of evidence required at the successive stages of the litigation").
194 *Lewert*, 819 F.3d at 968.
195 *Id.*

employees.[196] Following the theft of the laptop, Starbucks informed the affected employees and asked that they monitor their financial accounts and take steps to mitigate the risk of identity theft. Starbucks even provided affected employees with free credit monitoring services for one year.[197] A class of affected employees brought suit against the coffee chain, alleging an increased risk of future misuse of their personal information; in fact, one plaintiff alleged that someone had already attempted to open a bank account in his name but the bank had closed the account before he had suffered any losses.[198] The court held that the plaintiffs allegations constituted a legally cognizable threat of real and immediate harm from the theft of the store's laptop.[199] The court explained that while the plaintiffs' alleged injuries would have been too "conjectural or hypothetical" to find a credible threat of future injury had no laptop been stolen, their alleged injuries were real and imminent enough for a determination of standing because they premised their claim on the risk that the laptop would be stolen again in the future.[200]

In the more recent case of *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, the Ninth Circuit once again addressed standing in the data breach context.[201] The case was brought following a breach of Zappos' online retail servers, where hackers "allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of more than 24 million Zappos customers."[202] Zappos customers filed multiple putative class action suits in various federal courts, alleging that Zappos had not adequately protected their personal information. Importantly, the Ninth Circuit addressed the claims "based on the hacking incident itself, not any subsequent illegal activity."[203] The plaintiffs argued that the type of information the hackers obtained from the breach put them at imminent risk of identity theft.[204]

Relying on its holding in *Krottner*, the Ninth Circuit concluded that the *Zappos* plaintiffs had sufficiently alleged standing based on the risk

196 Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
197 *Id.* at 1141.
198 *Id.*
199 *Id.* at 1143.
200 *Id.*
201 *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019).
202 *Id.* at 1023.
203 *Id.*
204 *Id.* at 1023, 1027 ("Plaintiffs allege that the type of information accessed in the Zappos breach can be used to commit identity theft, including by placing them at higher risk of 'phishing' and 'pharming,' which are ways for hackers to exploit information they already have to get even more PII.").

of identity theft.[205] The court rejected Zappos' argument that *Krottner* was no longer good law post-*Clapper*, reasoning that *Krottner* was "not clearly irreconcilable with *Clapper*," and it therefore remained binding.[206] In assessing the plaintiffs' claims holistically and in light of *Krottner*, the court found that the *Zappos* plaintiffs had sufficiently alleged an injury-in-fact based on the substantial risk that the hackers would commit fraudulent acts or identity theft.[207] The court reasoned that the information stolen by the hackers in *Zappos* was "sufficiently similar" to the sensitive information contained on the stolen laptop in *Krottner*.[208] The *Zappos* plaintiffs alleged that their credit card numbers were also obtained in the breach, information that Congress itself had acknowledged is highly sensitive when it comes to the risk of identity theft.[209] Although there were no allegations that the hackers had obtained the plaintiffs' social security numbers, as was alleged in *Krottner*, the court explained that the information taken in this breach nevertheless gave the hackers the necessary tools to commit fraud or identity theft. The court viewed Zappos' suggestion to affected customers "to change their passwords on any other account where they may have used 'the same or similar password'" as evidence corroborating this explanation.[210]

To strengthen its reasoning, the court considered the allegations of the plaintiffs whose information had *already* been used for fraudulent purposes to be a refutation of Zappos' claim that the information breached could not be used to commit fraud or identity theft.[211] The court also rejected Zappos' contention that "too much time has passed since the breach for any harm to be imminent,"[212] holding instead that the timing of the breach is irrelevant to an assessment of standing because, when

[205] *Id.* at 1023.

[206] *Id.* at 1026 ("Unlike in *Clapper*, the plaintiffs' alleged injury in *Krottner* did not require a speculative multi-link chain of inferences. . . . The *Krottner* laptop thief had all the information he needed to open accounts or spend money in the plaintiffs' names—actions that *Krottner* collectively treats as 'identity theft.' . . . Moreover, *Clapper*'s standing analysis was 'especially rigorous' because the case arose in a sensitive national security context involving intelligence gathering and foreign affairs, and because the plaintiffs were asking the courts to declare actions of the executive and legislative branches unconstitutional. . . . *Krottner* presented no such national security or separation of powers concerns. And although the Supreme Court focused in *Clapper* on whether the injury was 'certainly impending,' it acknowledged that other cases had focused on whether there was a 'substantial risk' of injury." (internal citations omitted)).

[207] *Id.* at 1029.

[208] *Id.* at 1027.

[209] *Id.* ("Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft." (internal citation omitted)).

[210] *Id.*

[211] *Id.*

[212] *Id.* at 1028-29.

consumers' personal information is compromised, they may not see the full damage of the theft or fraud for years.[213]

G. *The D.C. Circuit*

In 2014, an unknown hacker breached health insurer CareFirst's database, which contained the unencrypted personally identifying health information of CareFirst's customers.[214] A class of the affected customers sued Carefirst, and the D.C. Circuit decided *Attias v. Carefirst, Inc.* in 2017. The court held that the plaintiffs possessed Article III standing based solely on the allegations that the theft of their personal information exposed them to increased risk of identity theft.[215] Significantly, the court found that the district court had erroneously concluded that the plaintiffs lacked standing based on an incorrect finding that there were no allegations that social security or credit card numbers were obtained in the breach.[216] The D.C. Circuit found that the *Attias* plaintiffs had, in fact, alleged the theft of that information.[217]

The *Attias* plaintiffs had specifically alleged that their names, dates of birth, email addresses, and subscribers' identification numbers had been stolen. Crucially to their case, they argued that the combination of this personal information yielded a substantial risk of "medical identity theft," in which "a fraudster impersonates the victim and obtains medical services in her name."[218] Because "medical identity fraud" could lead to severe consequences for victims, the court found this allegation alone—even absent any claims that social security or credit card numbers were stolen—created a very real possibility that the plaintiffs faced a dangerously high risk of identity theft.[219]

In characterizing the alleged risk of future harm to the *Attias* plaintiffs as "substantial," the court distinguished *Attias* from *Clapper*, where the Supreme Court held that the harm to the plaintiffs could *only* take place following an attenuated sequence of hypothetical events that

---

213 *Id.*

214 Attias v. Carefirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017).

215 *Id.* at 626; *see* Megan L. Brown et al., *D.C. Circuit Data Breach Standing Decision Will Encourage More Litigation Over Security in New Technology*, WILEY REIN LLP (Aug. 2017), https://www.wileyrein.com/newsroom-newsletters-item-PIF_August_2017-DC_Circuit_Data_Breach_Standing_Decision_Will_Encourage_More_Litigation_Over_Security_in_New_Technology.html [https://perma.cc/4ACA-9D6T].

216 *Attias*, 865 F.3d at 627.

217 *Id.* at 628 ("So we have specific allegations in the complaint that CareFirst collected and stored 'PII/PHI/Sensitive Information,' a category of information that includes credit card and social security numbers; that PII, PHI, and sensitive information were stolen in the breach; and that the data 'accessed on Defendants' servers' place plaintiffs at a high risk of financial fraud. The complaint thus plausibly alleges that the CareFirst data breach exposed customers' social security and credit card numbers.").

218 *Id.* at 628.

219 *Id.*

were not alleged to have occurred at the time the suit was brought. The *Clapper* Court had found that the harm to the plaintiffs depended on the actions of a series of independent actors—which made it less likely to predict how they would use the stolen information.[220] In *Attias*, the court distinguished the circumstances from *Clapper*, finding that an unauthorized party had *already* accessed personal information from the CareFirst database.[221] Thus, the court held that the harm to the plaintiffs was "much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill."[222] Given the fact that "[n]o long sequence of uncertain contingencies involving multiple independent actors" would have to occur before the *Attias* plaintiffs could suffer harm, the court concluded that there existed a substantial risk of harm merely from the sensitive nature of the information that was breached.[223]

CONCLUSION

Recent history has shown the increasing prevalence of data breaches that compromise millions of Americans' personal information. Continuing technological advances mean that the practice of storing personal information in databases will only continue to become more commonplace, and that hackers' ability to outsmart these systems will mimic such growth accordingly. Thus, the volume of data breaches is unlikely to slow down any time soon, and the most effective way to mitigate the harm they cause is through the enactment of a federal data breach law that provides sufficient protections to affected consumers.

Under our current system, entities that house consumer data are burdened with adherence to fifty-one widely varied state laws. Moreover, some federal jurisdictions—the Third, Fourth, and Eighth Circuits—require plaintiffs to allege more than a future risk of harm when hackers steal their personal, perpetually valuable information. The split in federal precedent leaves millions of consumers unable to take legal action against the entities who fail to protect their sensitive data. This lack of legal accountability leaves entities disincentivized from ensuring that they have adequate security measures in place. It is now time for a change.

Outside of the data breach context, courts have routinely recognized intangible harms as sufficient injuries to be litigated, often awarding current compensation to plaintiffs for potential future harms. There is no reason why it should remain different for data breach plaintiffs. The

220 *Id.*; *see* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410-14 (2013).
221 *Attias*, 865 F.3d at 628.
222 *Id*.
223 *Id.* at 629.

nature of the personal information stolen by hackers leaves victims, whose information has been breached but not yet misused, at a perpetually grave risk of harm. Adopting a federal law modeled after the California Act, which includes a broad definition of "injury," would substantially lower the standing threshold for data breach plaintiffs, thereby allowing all affected victims, whether they have been harmed or merely put at risk of future harm, to *at least* have their day in court. Moreover, freeing these victims from the heightened burden of establishing Article III standing would impose unfavorable consequences only on the entities who do not take due care in protecting their consumers' personal, perpetually valuable information.

Importantly, the case law emanating from the Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits provides overwhelming evidence as to why allegations of future injury by data breach plaintiffs pass constitutional muster. Allowing plaintiffs to assert claims based on a substantial risk of future harm—often accompanied by the present injury of mitigation costs incurred to lessen that future harm—does not run afoul of Article III's case or controversy requirement. Therefore, in the wake of the Supreme Court's recent denial of the opportunity to guide the standing inquiry in data breach cases, Congress must step in and give data breach victims a chance at the legal recourse they deserve.

California understands the issue for consumers at the heart of the data breach problem and has already implemented a consumer-friendly remedy by lowering the standing threshold. This allows victims who face real risk, and the accompanying reasonable fears about the misuse of their data, to have their day in court. In turn, entities are encouraged to put into place adequate security measures to avoid liability. While many of the other fifty laws currently in play are consumer-friendly, waiting for those states to follow California's action would be a mistake. *All* American consumers deserve the assurance that their personal information will be protected and that there will be consequences for those who fail to do so.

Gabriela Nastasi[*]

[*] Staff Editor, *Cardozo Arts & Entertainment Law Journal* Vol. 37, J.D. Candidate, Benjamin N. Cardozo School of Law (2020); B.A., Communication, Minor, American Studies, concentration: law, politics, and culture, Boston College (2017). I would like to thank Professor David Rudenstine, whose invaluable wisdom and guidance made this Note possible, and whose passion for constitutional law will forever inspire me. I would also like to thank my parents, Caroline and Anthony, and my brother and sister, Frankie and Victoria, for their unconditional love, patience, and support throughout my law school career. Because of you, I am living my dream.