Golden Gate University Law Review

Volume 52 | Issue 2 Article 5

November 2022

COMMENT: INJURY-IN-FACT: SOLVING THE FEDERAL CIRCUIT COURT SPLIT REGARDING CONSTITUTIONAL STANDING IN DATA THEFT LITIGATION

Simone Cadoppi

COMMENT

INJURY-IN-FACT: SOLVING THE FEDERAL CIRCUIT COURT SPLIT REGARDING CONSTITUTIONAL STANDING IN DATA THEFT LITIGATION

*SIMONE CADOPPI**

INTRODUCTION

Data theft from cyber threats is a developing problem in our increasingly digitized world.[1] Data theft can cause the exposure of sensitive records and lead to losses of millions of dollars to both businesses and individuals.[2] Victims of data breaches often bring suits against companies that fail to properly safeguard personal information, with hopes that courts will redress their harms.[3] These victims often encounter problems during the initial stages of their cases when attempting to establish their right to sue—also known as constitutional standing.[4] One such problem is that the Supreme Court of the United States has not resolved whether the victims of data breaches have standing to sue for the threat of future

* J.D. Candidate, Golden Gate University School of Law, May 2022; B.A. History, San Francisco State University, May 2015. The author would like to thank the entire 2020–2021 and 2021–2022 *Golden Gate University Law Review* staffs and Professor David Franklyn for their diligent feedback and unwavering support during the writing of this piece. The author also gives special thanks to Stefano Cadoppi, Carole Cadoppi, Adrian Cadoppi, and Dario Cadoppi, without whom none of this would be possible.

[1] *See* Tom Burt, *Microsoft Report Shows Increasing Sophistication of Cyber Threats*, MICROSOFT ON THE ISSUES (Sept. 29, 2020), https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/.

[2] Maddie Davis, *4 Damaging After-Effects of a Data Breach*, CYBINT (July 25, 2019), https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/.

[3] *See Data Breach Lawsuit*, CLASSACTION.COM (Nov. 30, 2018), https://www.classaction.com/data-breach/lawsuit/.

[4] 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.

harm stemming from stolen data.[5] This lack of guidance by the Supreme Court has resulted in a federal circuit court split about whether a risk of future harm of identity theft is sufficient to satisfy the constitutional requirement of standing.[6]

This Comment explores the circuit split with regard to standing in data theft cases and proposes a solution for the Supreme Court to adopt. Specifically, the federal circuit courts are divided between a more permissive "substantial risk" standard and a more prohibitive "certainly impending" standard.[7] To resolve this split, the Supreme Court should adopt the more permissive substantial risk standard that only requires plaintiffs to show that there exists a substantial risk of future harm stemming from an actual data breach.[8] Furthermore, when establishing constitutional standing, the Supreme Court should only require that plaintiffs establish the occurrence of an actual data breach that resulted in the theft of sensitive information. Part I provides background on data theft and its increasing prevalence. Part II discusses the elements required to establish constitutional standing, and how they are analyzed in the context of allegations of threats of future harm. Part III compares historical cases that have applied a permissive standard to evaluate threats of future harm with cases that have done so using a more prohibitive standard. Part IV compares the most recent cases examining the threat of future harm and evaluates the current status of the circuit split regarding this issue. Part V proposes a new standard for the Supreme Court to adopt to resolve the circuit split in data breach cases alleging a risk of future harm.

I. THE HISTORICAL BACKGROUND OF DATA THEFT

Data breaches were first recorded in 2005 by Privacy Rights Clearing House.[9] The DSW Shoe Warehouse data breach in 2005, which compromised approximately 1.4 million credit card names and numbers, was

[5] Bradford C. Mank, Article, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1362-63 (2017).

[6] *Id*.

[7] *See Second Circuit Seeks to Reconcile Circuit Split Concerning Standing to Bring Data Privacy Lawsuits*, GIBSONDUNN (April 30, 2021), gibsondunn.com/second-circuit-seeks-to-reconcile-circuit-split-concerning-standing-to-bring-data-privacy-lawsuits/.

[8] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 164 (2014).

[9] J. Charlton Collins, *Check on Data Breaches at the Privacy Rights Clearinghouse*, JOURNAL OF ACCOUNTANCY (Sept. 1, 2019), https://www.journalofaccountancy.com/issues/2019/sep/data-breaches-privacy-rights-clearinghouse.html.

one of the first major data breaches in the United States.[10] Subsequently, in 2005, 157 data breaches exposed almost 67 million sensitive records.[11]

Data is commonly classified as either sensitive or non-sensitive.[12] In general, sensitive data reveals financial or health data, or personal information subject to regulations.[13] Non-sensitive data includes information that is a matter of public record or routine business information that is openly shared, such as information contained in "cookies."[14]

In 2009, 498 data breaches exposed over 222 million sensitive records. Further, in 2015 those numbers rose to 784 data breaches which exposed over 169 million sensitive records.[15] The next few years witnessed an even more staggering increase in data breaches and exposed records.[16] Data breaches from 2017 to 2019 exposed over 833 million sensitive records, including a whopping 1,257 breaches exposing 471 million sensitive records in 2018 alone.[17] When combined, the volume of both sensitive and non-sensitive records lost to data theft is even more alarming. In 2017 alone, almost 3.5 billion records were stolen.[18]

What do cyber criminals do with stolen data? Stolen data is commonly used for data ransom, dark web sales, and identity theft.[19] Data

---

[10] *Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, https://privacyrights.org/data-breaches (last visited Nov. 23, 2020).

[11] Joseph Johnson, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, STATISTA (March 3, 2021), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.

[12] *See GDPR Sensitive and Non-Sensitive Data: A Distinction With a Difference*, CRITEO (Dec. 21, 2017), https://www.criteo.com/blog/gdpr-sensitive-non-sensitive-data-distinction-difference/.

[13] Examples of personal information subject to regulations include: racial or ethnic origin, political opinion, religious or philosophical beliefs, genetic data, or classified information. Abi Tyas Tunggal, *What is Sensitive Data?*, UPGUARD (Aug. 27, 2020), https://www.upguard.com/blog/sensitive-data; Rob Sobers, *2019 Data Risk Report Stats and Tips You Won't Want to Miss*, VARONIS (Jun. 17, 2020), https://www.varonis.com/blog/data-risk-report-highlights-2019/.

[14] Abi Tyas Tunggal, *What is Sensitive Data?*, UPGUARD (Aug. 27, 2021), https://www.upguard.com/blog/sensitive-data; *See Archived: What are Cookies?*, KNOWLEDGEBASE (Jan. 18, 2018), https://kb.iu.edu/d/agwm (Defining Cookies as "messages that web servers pass to your web browser when you visit Internet sites.") ("These files typically contain information about your visit to the webpage, as well as any information you've volunteered, such as your name and interests.")

[15] Joseph Johnson, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, STATISTA (Mar. 3, 2021), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[16] *Id.*

[17] *Id.*

[18] Manisha Verma, *The Data Behind Data Breaches: What 7 Charts Tell Us*, THOUGHTSPOT, (Oct. 10, 2018), https://www.thoughtspot.com/thoughtspot-blog/data-behind-largest-data-breaches-what-7-charts-tell-us-thoughtspot.

[19] *What do Hackers do with your stolen data?*, SABIO INFORMATION TECHNOLOGIES (May 15, 2018), http://www.sabioit.com/2018/05/15/hackers-stolen-data/.

ransom, carried out by ransomware,[20] refers to cyber-attacks that block companies and individuals from accessing their files, databases, and other computer systems until a ransom is paid.[21] Between 2015 and 2021, ransomware damages have increased from $325 million to a projected $20 billion.[22] By 2031, ransomware is expected to cost its victims approximately $265 billion, annually.[23] Cyber criminals have used ransomware to attack everything from schools and businesses to healthcare providers and municipalities.[24]

Cybercriminals also commonly sell stolen data on the dark web[25]—an area of the internet only accessible by using specific software that protects users' identities and locations with encryption technology, making users difficult to track.[26] The volume of stolen usernames and passwords circulating the dark web has increased by 300% since 2018, resulting in over 15 billion stolen account login credentials, including usernames and passwords for online banking, social media accounts, and streaming services.[27] Cybercriminals stand to make a lot of money when considering the value and amount of stolen credentials on the dark web.[28] For example, credit cards average $33.88 per credential, forged documents can net between $70 and $1500, G-mail accounts are worth about $155, and social media accounts, such as Twitter, start at $49.[29]

---

[20] "Ransomware is a form of malware that encrypts a victim's files." Josh Fruhlinger, *Ransomware Explained: How it Works and How to Remove It*, CSO (June 19, 2020), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

[21] Casey Crane, *20 Ransomware Statistics You're Powerless to Resist Reading*, HASHEDOUT (Feb. 27, 2020), https://www.thesslstore.com/blogC/ransomware-statistics/.

[22] *Id.*

[23] David Braue, *Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031*, CYBER SECURITY VENTURES (Jun. 3, 2021), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[24] Casey Crane, *20 Ransomware Statistics You're Powerless to Resist Reading*, HASHEDOUT (Feb. 27, 2020), https://www.thesslstore.com/blog/ransomware-statistics/.

[25] *See* Davey Winder, *Hacker Gives Away 386 Million Stolen Records On Dark Web—What You Need To Do Now,* FORBES (July 29, 2020, 5:15 AM), https://www.forbes.com/sites/daveywinder/2020/07/29/hacker-gives-away-386-million-stolen-records-on-dark-web-what-you-need-to-do-now-shinyhunters-data-breach/?sh=4c2ae496f395.

[26] Photon Research Team, *Dark Web Monitoring: The Good, The Bad, and The Ugly*, DIGITAL SHADOWS (Sept. 11, 2019), https://www.digitalshadows.com/blog-and-research/dark-web-monitoring-the-good-the-bad-and-the-ugly/.

[27] Davey Winder, *New Dark Web Audit Reveals 15 Billion Stolen Logins from 100,000 Breaches*, FORBES (Jul. 8, 2020), https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=79c0cffc180f.

[28] Charlie Osbourne, *Over 23 Million Stolen Credit Cards are Being Traded on the Dark Web*, ZDNET (July 29, 2019), https://www.zdnet.com/article/over-23-million-stolen-credit-cards-are-being-traded-on-the-dark-web/.

[29] *Average Price of Stolen Credentials on Dark Web Marketplaces as of February 2019*, STATISTA (Nov. 23, 2020), https://www.statista.com/statistics/1007470/stolen-credentials-dark-web-

One of the most common results of data breaches is identity theft.[30] The 1998 Identity Theft and Assumption Deterrence Act defined identity theft as "the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime."[31] In 2005, the U.S. Bureau of Statistics reported that 6.4 million households experienced one or more types of identity theft, resulting in financial losses of over $11 billion.[32] In 2016, the Bureau reported that at least 17.7 million consumers were victims of identity theft, resulting in financial losses of approximately $17.5 billion.[33]

A 2018 study by the White House's Council of Economic Advisors revealed that in 2016, malicious cyber activity[34] cost the economy between $57 billion and $109 billion.[35] Not only does data theft negatively impact the economy, but stolen data affects both individuals and businesses alike.[36] Theft of consumer and business information is a steadily growing trend and a lucrative business for cybercriminals.[37] As such, it is imperative that victims of data theft be able to redress their harms in court, which requires them to establish their right to stand before the court, also known as standing.

II. STANDING

The Constitution vests the judicial powers of the United States in the federal courts,[38] with jurisdiction limited to "cases" and "controver-

---

market-price/; *See also* Miguel Gomez, *Dark Web Price Index 2020*, PRIVACY AFFAIRS (Oct. 3, 2020), https://www.privacyaffairs.com/dark-web-price-index-2020/.

[30] Matt Tatham, *Identity Theft Statistics*, EXPERIEN (Mar. 15, 2018), https://www.experian.com/blogs/ask-experian/identity-theft-statistics/.

[31] William Roberds & Stacey L. Schreft, *Data Security, Privacy, and Identity Theft: The Economics Behind the Policy Debates*, FED. RESV. BANK OF CHI. 22, 22 (2009), https://www.chicagofed.org/-/media/publications/economic-perspectives/2009/ep-1qtr2009-part4-roberds-schreft-pdf.pdf.

[32] Katrina Baum, U.S DEPARTMENT OF JUST., BUREAU OF JUSTICE STATISTICS SPECIFIC REPORT at 1 (2019), https://www.bjs.gov/content/pub/pdf/it05.pdf.

[33] Erika Harrel, U.S DEPARTMENT OF JUST., BUREAU OF JUSTICE STATISTICS SPECIFIC REPORT at 1, 1 (2019), https://www.bjs.gov/content/pub/pdf/it05.pdf.

[34] THE COUNCIL OF ECONOMIC ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY at 3, (2018), https://www.hsdl.org/?view&did=808776, (defining malicious cyber activity as "an activity, other than one authorized by or in accordance with U.S. law, that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident thereon").

[35] *Id.*

[36] *Id.*

[37] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

[38] U.S. CONST. art. III, § 1.

sies."[39] An "essential and unchanging" part of the Article III case and controversy requirement is standing.[40] To establish standing, a plaintiff must show the "irreducible constitutional minimum" of standing's three elements: (1) an "injury-in-fact," (2) causation, and (3) a likelihood of redressability.[41] Establishing an injury-in-fact is currently the most contested element in data theft cases.[42]

An injury-in-fact "is an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not 'conjectural' or 'hypothetical.'"[43] The injury-in-fact requirement of constitutional standing is generally a difficult element to prove in data breach cases because it takes time for stolen data to eventually be used for nefarious purposes.[44] Since the risk of future harm is not an actual injury, as the harm has not yet occurred, it must satisfy the imminence requirement of Article III standing. The imminence requirement has shown to be a major roadblock to litigants alleging a future risk of harm, especially where the alleged threat of future harm is identity theft.[45]

A. RECENT DECISIONS SHAPING THE "IMMINENCE" ELEMENT OF INJURY-IN-FACT

A future injury satisfies the injury-in-fact requirement only where the future injury is imminent. This section examines—through two cases—two standards to evaluate the imminence of a future harm: certainly impending and substantial risk.[46] In *Clapper v. Amnesty International*, the Court held that the plaintiff alleged a future injury that was

[39] U.S. CONST. art. III, § 2, cl. 1; *The Two Classes of Cases and Controversies*, LAW CORNELL (Mar. 9, 2021), https://www.law.cornell.edu/constitution-conan/article-3/section-2/clause-1/the-two-classes-of-cases-and-controversies (Defining cases and controversies as "the claims of litigants brought before the courts for determination by such regular proceedings as are established by law or custom for the protection or enforcement of rights, or the prevention, redress, or punishment of wrongs.").

[40] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

[41] *Id.* at 61.

[42] Nancy R. Thomas, *No Injury, No Data Breach Claims? Depends on the Circuit*, MORRISON FOERSTER (Sept. 17, 2020), https://www.mofo.com/resources/insights/200917-no-data-breach-claims.html.

[43] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-560 (1992).

[44] Priscilla Fasoro & Lauren Wiseman, Standing Issues in Data Breach Litigation: An Overview, COVINGTON (Dec. 7, 2018), https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/.

[45] Edward P. Boyle, Emilio W. Cividanes, & Stuart P. Ingis, *The Impact of the Supreme Court's Recent Decision In Clapper v. Amnesty International USA on Privacy and Data-Security Litigation*, VENABLE (Mar. 2013), https://www.venable.com/insights/publications/2013/03/the-impact-of-the-supreme-courts-recent-decision-i.

[46] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); Susan B. Anthony List v. Driehaus, 573 U.S. 149 (2014).

too speculative to satisfy the imminence element of the injury-in-fact requirement.[47] Section 702 of the Foreign Intelligence Surveillance Act ("FISA") of 1978 allows the U.S. government to conduct surveillance of individuals "who are not 'United States persons' and are reasonably believed to be located outside the United States."[48] The plaintiffs' work required them to engage in sensitive communications with individuals whom they expected to be likely targets of FISA surveillance.[49] The plaintiffs claimed an injury-in-fact that stemmed from the objectively reasonable likelihood that their communications would be acquired "at some point in the near future."[50]

The Court did not find the plaintiffs' injury-in-fact argument convincing, holding that their theory of future injury was too speculative to be considered certainly impending.[51] The Court characterized the plaintiff's theory of standing as a "highly attenuated chain of possibilities" that should not be considered certainly impending.[52] However, the Court acknowledged that plaintiffs do not have to be "literally certain that the harms they identif[ied] will come about."[53] The Court explained how they have found standing in some situations where there existed a substantial risk of future harm.[54]

The Court in *Susan B. Anthony List v. Driehaus* held that a plaintiff had established the injury-in-fact element by showing a substantial risk of future harm.[55] Plaintiff Susan B. Anthony List ("SBA") was a pro-life organization that criticized members of Congress for their votes supporting a tax-payer funded abortion bill during a political campaign.[56] SBA attempted to erect a billboard condemning a congressman for his vote, a billboard that was never displayed after the congressman threatened the company that owned the billboard space with legal action.[57] The congressman filed a complaint with the Ohio Elections Commission, alleging that SBA had violated a statute that prohibited false statements made during any campaign for nomination or election to public office or office of a political party.[58] The Congressman's suit was dismissed, but SBA

[47] *Id.* at 401.
[48] *Id.*
[49] *Id.*
[50] *Id.*
[51] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).
[52] *Id.* at 410.
[53] *Id.* at 414.
[54] *Id.*
[55] Susan B. Anthony List v. Driehaus, 573 U.S. 149, 164 (2014).
[56] *Id.* at 153-54.
[57] *Id.* at 154.
[58] *Id.*

challenged the constitutionality of the statute on First Amendment grounds.[59]

SBA argued that the statute "chilled" their speech, that SBA planned "to engage in substantially similar activity in the future," and that they therefore faced the prospect of future injury—the "prospect of its speech and associational rights again being chilled and burdened."[60] The Court upheld the plaintiff's standing because "the threat of future enforcement of the false statement statute is *substantial*."[61] Importantly, the Court elected to use the substantial risk standard rather than the certainly impending standard used in *Clapper*, signifying that both of the standards of future injury are valid to establish an injury-in-fact.[62]

B. CLARIFICATION OF THE "CONCRETENESS" ELEMENT OF INJURY-IN-FACT

In *Spokeo v. Robbins,* the Court further clarified earlier dicta that an injury-in-fact must be *both* "concrete and particularized."[63] This decision resulted in a stricter standard for the injury-in-fact element.[64] Previously, courts analyzed concreteness and particularization together, as the Court of Appeals for the Ninth Circuit did in *Spokeo* prior to its appeal to the Supreme Court.

Spokeo is a company that operates a search engine that allows users to input information and search a wide variety of databases that provides users with information on individuals.[65] Spokeo was used to perform a search on plaintiff Robbins, which resulted in the garnering and dissemination of inaccurate information.[66] Robbins filed suit alleging that Spokeo willfully failed to comply with the Fair Credit Reporting Act of 1970, which 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."[67]

The Supreme Court reviewed the plaintiff's complaint and clarified the "concrete" and "particularized" standard for establishing the injury-

---

[59] *Id.* at 155.

[60] *Id.*

[61] *Id.* at 164.

[62] *Id*. 158-164.

[63] Spokeo v. Robbins, 136 S. Ct. 1540, 1545 (2016).

[64] *Spokeo's Implications for Cyber-Security Litigation*, HUGHES HUBBARD (last visitied, Nov. 4, 2021), https://www.hugheshubbard.com/news/ealert-spokeos-implications-for-cyber-security-litigation.

[65] Spokeo v. Robbins, 136 S. Ct. 1540, 1544 (2016).

[66] *Id.*

[67] Spokeo v. Robbins, 136 S. Ct. 1540, 1542-43 (2016).

in-fact element. An injury is considered particularized if it "affect[s] the plaintiff in a personal and individual way."[68] "A 'concrete' injury must be 'de facto'; that is, it must actually exist."[69] However, the Court did not synonymize "concrete" with "tangible," affirming that intangible injuries can be concrete.[70] Most importantly, the Court stated that a real risk of harm *can* satisfy concreteness,[71] meaning that the imminence standard for future harm expounded upon in *Clapper* and *Susan B. Anthony* is connected with and may be sufficient for a finding of concreteness.

III. INJURY-IN-FACT IN DATA BREACH CASES

Prior to the Supreme Court's attempts in *Clapper and Spokeo* to clarify standing in data breach cases, federal circuit courts were split on whether a risk of future harm could satisfy the injury-in-fact element of standing, and the degree of future harm that would achieve that result. To interpret the injury-in-fact requirement, circuit courts developed two distinct approaches—the permissive, plaintiff-friendly approach, and the prohibitive, defendant-friendly approach.

A. THE PERMISSIVE APPROACH

The Court of Appeals for the Seventh and Ninth Circuits developed a permissive and inclusive standard when identifying which injuries would satisfy the injury-in-fact requirement.[72] For example, the courts in *Pisciotta v. Old National Bancorp* and *Krottner v. Starbucks Corp.* held that an increased risk of future harm is sufficient to satisfy the injury-in-fact requirement.

The court in *Pisciotta* held that the injury-in-fact requirement could be satisfied by an increased risk of future harm.[73] Old National Bancorp ("ONB") operated a website where prospective customers could apply for accounts, loans, and other ONB services online.[74] Online applications required users to input customer names, addresses, social security numbers, driver's license numbers, dates of birth, and credit card or other financial account information.[75] After a breach of ONB's website, plain-

[68] *Id.* at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 n. 1 (1992)).
[69] *Id.* at 1548.
[70] *Id.* at 1549.
[71] *Id.*
[72] Kristen L. Bryan, *Denied! Federal Court Allows Claims to Proceed Concerning Wide Scale Data Breach,* NAT'L LAW REV. (Nov. 23, 2020), https://www.natlawreview.com/article/denied-federal-court-allows-claims-to-proceed-concerning-wide-scale-data-breach.
[73] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).
[74] *Id.* at 631.
[75] *Id.*

tiffs filed a putative class action alleging that ONB failed to adequately protect the consumers' personal information and that the plaintiffs would suffer a future threat of injury.[76] Despite a failure to allege any "direct financial losses"[77] as a result of the data breach, the court held that the injury-in-fact element could be satisfied in two ways: by showing a threat of future harm, or by showing an act which increases the risk of future harm.[78]

The court in *Krottner* also held that alleging an increased risk of future injury may satisfy the injury-in-fact element.[79] In *Krottner*, thieves stole a laptop containing unencrypted names, addresses, and social security numbers of approximately 97 thousand Starbucks employees.[80] Although the plaintiffs did not allege that the stolen data had been misused, the court still found that the injury-in-fact element was met based on a "credible threat of real and immediate harm" stemming from the stolen unencrypted personal data.[81] The Court of Appeals for the Ninth Circuit agreed with the plaintiff's allegation that an increased risk of future identity theft was sufficient for a finding of injury-in-fact and that the plaintiff satisfied standing.

B. THE PROHIBITIVE APPROACH

In *Reilly v. Ceridian Corp.*, the Court of Appeals for the Third Circuit took a more restrictive view of the injury-in-fact requirement. The key distinction between *Reilly* and the more lenient holdings in *Pisciotta* and *Krottner* is that the Third Circuit in *Reilly* required evidence of misuse or malicious intent of breached data to establish an injury-in-fact.[82]

In *Reilly*, the court held that the Appellants' allegations of future injury were too speculative to establish standing.[83] Ceridian is a payroll processing company that collects its customers' and employees' information for operational purposes.[84] This information includes employees' names, addresses, social security numbers, dates of birth, and bank account information.[85] A hacker gained access to Ceridian's system and potentially accessed the personal and financial information of approxi-

[76] *Id.* 632.
[77] *Id.*
[78] *Id.* 634.
[79] *Id.* 1143.
[80] Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
[81] *Id.* at 1143.
[82] Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011).
[83] *Id.* at 46.
[84] *Id.* at 40.
[85] *Id.*

mately 27 thousand employees at 1,900 companies.[86] However, Ceridian could not determine whether the hacker "read, copied, or understood the data."[87]

The court held that the Appellants' allegations of a "hypothetical, future injury [did] not establish standing under Article III."[88] The court reasoned that the Appellants' contentions relied on a speculative chain of events that was too attenuated to establish an injury-in-fact; a chain of events requiring that the hacker "(1) read, copied, and understood their personal information; (2) intend[d] to commit future criminal acts by misusing the information;" and (3) possess the ability to use such information to the detriment of the Appellants.[89] Thus, the court deemed the risk of future injury too speculative to rise to the level of a certainly impending threat.[90]

The court distinguished *Reilly* from *Pisciotta* and *Krottner* in that the threatened harms in the latter two cases were significantly more imminent and certainly impending than they were in *Reilly*.[91] In *Pisciotta*, the court emphasized the existence of evidence showing that the hacker's intrusion was sophisticated and malicious.[92] In *Krottner*, the court highlighted the fact that someone attempted to open a bank account with the plaintiff's information following the theft.[93] By contrast, the court in *Reilly* found that the absence of evidence showing malicious intent or misuse meant that the "string of hypothetical injuries" were insufficient to establish that the plaintiffs had suffered either an actual or imminent injury.[94]

IV. The Federal Circuit Split: Whether a Risk of Future Harm Satisfies The Injury-in-Fact Requirement

Despite *Clapper*, the federal circuit court split regarding whether a risk of future harm satisfies the injury-in-fact requirement remains. The following cases reflect the differing opinions on this issue, which have yet to be resolved by the Supreme Court. The circuit split reflects two opposing approaches: a defendant-friendly approach, and a plaintiff-friendly approach.

---

[86] *Id.*
[87] *Id.*
[88] *Id.* 41.
[89] *Id.*
[90] *Id.* at 43.
[91] *Id.* at 44.
[92] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).
[93] Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011).
[94] *Id.*

A. THE DEFENDANT-FRIENDLY APPROACH

The First, Second, Fourth, and Eighth Circuit courts have all championed a defendant-friendly approach to the injury-in-fact analysis concerning whether a future risk of harm from stolen personal information is substantial or a certainly impending.

1. The Fourth Circuit: Beck v. McDonald

In *Beck v. McDonald*, the Court of Appeals for the Fourth Circuit used a restrictive interpretation of the injury-in-fact requirement. Although the facts in *Beck* resemble those in *Krottner*—the stolen laptop case—the Fourth Circuit arrived at a different result from the Ninth Circuit's decision in *Krottner*.

Plaintiffs in *Beck* received medical treatment and health care at a hospital that experienced two data breaches.[95] A laptop containing unencrypted information of approximately 7,400 patients was misplaced or stolen from a hospital.[96] The unencrypted data on this laptop included "names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight)."[97] An internal investigation showed that the hospital failed to follow the policies and procedures for handling a non-encrypted laptop that stored patient information.[98]

As in *Krottner*, the plaintiffs' alleged injury was a future threat of identity theft.[99] First, the court applied the certainly impending standard for imminence.[100] The Fourth Circuit held that for the plaintiffs to have suffered an injury, the court must "engage with the same attenuated chain of possibilities" that was rejected in *Clapper*.[101] Notably, the court considered persuasive the plaintiffs' failure to establish the thieves' intent to steal information.[102] In other words, the court valued and analyzed the thieves' intent—whether the thieves' intended simply to steal a laptop, or to steal the data in the laptop.[103]

Next, the court applied the substantial risk standard for imminence and arrived at the same result.[104] Here, the court analyzed the plaintiffs'

---

[95] Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).
[96] *Id.* at 267.
[97] *Id.*
[98] *Id*.
[99] *Id.* at 267-268.
[100] *Id.* at 268.
[101] *Id.* at 275
[102] *Id.* at 274-275.
[103] *Id.*
[104] *Id.* at 275.

contention that 33% of those affected by the data breach would become victims of identity theft.[105] Surprisingly, the court established a bright line rule, saying that data breaches resulting in the identity theft of 33% of those affected "falls far short" of establishing a substantial risk of harm.[106]

Thus, *Beck* is notable for four reasons. First, the *Beck* court considered noteworthy the intent of the thieves.[107] Second, the court considered *Clapper* as controlling over *Beck*, which shares the same type of facts with *Krottner* and *Pisciotta*.[108] Third, the court not only applied the substantial risk standard, but held that data breaches resulting in the identity theft of 33% of those affected "falls far short" of meeting the standard.[109] Fourth, the court considered the elapsed time from a data breach as indicative of whether an injury is merely speculative.[110]

2. The Eighth Circuit: In re SuperValu, Inc.

The Court of Appeals for the Eighth Circuit in *In re SuperValu Inc.* held that the risk of harm from identity theft did not establish a substantial risk sufficient to establish standing.[111] Defendant SuperValu Inc., an operator of retail grocery stores, suffered multiple data breaches resulting in the theft of customer information.[112] Over a period of almost a month, cybercriminals accessed the defendant's computer network that processes payment card transactions for 1,045 of the defendant's stores.[113] The hackers installed malware into the defendant's network that gave them access to customer names, credit or debit card account numbers, expiration dates, card verification value codes, and PIN numbers.[114]

The plaintiffs, a group of consumers who shopped at defendant's stores, claimed that the defendants failed to adequately protect consumer card information.[115] As a result, hackers gained access to their credit card information.[116] The plaintiffs' alleged injury-in-fact was a risk of future

---

[105] *Id.* at 275-276.

[106] *Id.* 276.

[107] *Id.*at 274.

[108] *Id.* at 275.

[109] *Id.* at 276.

[110] Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (Holding that "as the breaches fade further into the past, the Plaintiffs' threatened injuries become more and more speculative.").

[111] *In re* SuperValu, Inc., 870 F.3d 763, 771 (8th Cir. 2017).

[112] *Id.* at 765.

[113] *Id.* at 766.

[114] *Id.*

[115] *Id.*

[116] *Id.*

identity theft as a result of the data breach.[117] After acknowledging that either the substantial risk or the certainly impending standard could be used to find standing, the Eighth Circuit ultimately elected to analyze this case under the substantial risk standard.[118] The court held that the risk of concrete harm from identity theft was not substantial.[119]

In arriving at its holding, the court relied on the 2007 United States Government Accountability Office ("GAO") report on data breaches.[120] Guided by the GAO report, the court determined that stolen credit card information, without other information such as social security numbers, is generally insufficient to open unauthorized new accounts.[121] As a result, the court concluded that there was little to no risk that the stolen credit card information would be used for "the type of identity theft generally considered to have a more harmful direct effect on consumers."

Next, in an attempt to establish a substantial risk of harm, the court asked whether stolen credit card numbers could result in credit or debit card fraud.[122] The GAO report did not "plausibly support the contention that consumers affected by a data breach face a substantial risk of credit or debit card fraud."[123] The court cited passages from the GAO report declaring that the best available evidence indicated that most data breaches do not result in detected identity theft.[124] For example, "[b]ecause the report finds that data breaches are unlikely to result in account fraud, it does not support the allegation that defendants' data breaches create a substantial risk that plaintiffs will suffer credit or debit card fraud."[125]

Thus, *SuperValu* illustrates the fundamental difference in reasoning evident in the circuit split. As with the holding in *Beck*, the defendant-friendly circuit courts do not find a substantial risk of injury when evaluating stolen credit card information. Conversely, the plaintiff-friendly circuit courts regard stolen credit card information as evidence of a substantial risk of injury.[126]

---

[117] *Id.* at 768-69.

[118] *Id.* at 769.

[119] *Id.* at 771.

[120] *Id.* at 767.

[121] *Id.* at 770.

[122] *Id.*

[123] *Id.* at 771.

[124] *Id.*

[125] *Id.*

[126] *See infra* Part V, Section B.

B. THE PLAINTIFF-FRIENDLY APPROACH

The Court of Appeals for the District of Columbia and the Third, Sixth, Seventh, and Ninth Circuits have all championed a plaintiff-friendly approach to the injury-in-fact analysis when determining whether a future risk of harm due to stolen personal information is a substantial risk or a certainly impending risk.

1. The Seventh Circuit: Remijas v. Neiman Marcus Group

In *Remijas v. Neiman Marcus Group*, the court held that the risk of future harm was substantial, and therefore was both consistent with *Clapper* and sufficient to establish an injury-in-fact.[127] Here, hackers stole credit card information of the approximately 350,000 customers of the luxury department store Neiman Marcus.[128] The plaintiffs filed a complaint alleging a number of theories for relief, including negligence and violations of data breach laws.[129] Among other actual injuries, the plaintiffs alleged standing based on "two imminent injuries: an increased risk of future fraudulent charges and greater susceptibility to identity theft."[130] The court agreed with the plaintiffs.[131]

The Seventh Circuit distinguished *Remijas* from *Clapper* in that *Clapper* addressed speculative thefts that may never occur.[132] By contrast, in *Remijas*, the personal information had already been stolen.[133] Furthermore, approximately 9,200 of the 350,000 stolen credit card numbers had already experienced fraudulent charges.[134]

The court inferred a substantial risk of harm in part from the apparent intent of the data breach.[135] The court presumed that the purpose of the data breach was to make fraudulent charges or to assume the customers' identities, because "[w]hy else would hackers break into a store's database and steal consumers' private information?"[136]

Lastly, the Seventh Circuit opined that plaintiffs eventually may not be able to "provide an adequate factual basis" for their claims that remain at risk of harm for any extended period of time. The court noted how-

[127] Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).
[128] *Id.* at 689-90.
[129] *Id.* at 693.
[130] *Id.* at 692.
[131] *Id.* at 697.
[132] *Id.* at 692-93.
[133] *Id.* at 692.
[134] *Id*. at 690.
[135] *Id.* at 693.
[136] *Id.*

ever, that this eventuality was not the proper burden at the current stage in the pleadings.[137]

2. The Ninth Circuit: In re Zappos.com, Inc.

In *In re Zappos.com, Inc.*, the court held that where data thieves steal the type of information that will allow them to commit identity theft, the plaintiffs may establish standing by alleging threat of future harm.[138] Hackers breached online retailer Zappos.com, Inc.'s ("Zappos") servers, stealing "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."[139] Several customers filed a class action suit against Zappos asserting that Zappos had not properly protected their personal information.[140] The plaintiffs alleged that the data breach put them at an increased risk of harm from identity theft.[141]

First, the Ninth Circuit analyzed whether *Krottner* was still good law in light of the Supreme Court's decision in *Clapper*.[142] The court determined that *Krottner* is reconcilable with *Clapper*.[143] The court distinguished *Krottner* from *Clapper* in two ways. First, as opposed to *Clapper*, the alleged injury in *Krottner* did not require a speculative and attenuated chain of inferences.[144] And second, that the standing analysis in *Clapper* was especially rigorous because the case arose in a "sensitive national security context."[145]

Next, the court established that *Krottner* controlled *Zappos*.[146] In *Krottner*, the Ninth Circuit ruled that the sensitivity of the stolen information combined with its theft indicated an "adequately alleged injury-in-fact supporting standing."[147] Here, the stolen information was the same, but in addition full credit card numbers were stolen.[148] However, unlike the victims in *Krottner*, the victims in *Zappos* did not have their social security numbers stolen.[149] The court referred to congressional

[137] *Id.* at 694.
[138] *In re* Zappos.com, Inc., 888 F.3d 1020, 1029-30 (9th Cir. 2018).
[139] *Id.* at 1023
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.* 1026-1027.
[144] *Id.* at 1026.
[145] *In re* Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018) (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (9th Cir. 2013)).
[146] *In re* Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018).
[147] *Id.* at 1027 (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010)).
[148] *Id.* at 1023, 1027.
[149] *Id.* at 1027.

legislation preventing the printing of credit card numbers on receipts in an attempt to curb identity theft to support its finding that the stolen credit card information gave the "hackers the means to commit fraud or identity theft."[150]

Thus, in *Zappos*, the Ninth Circuit established that stolen personal identifying information and credit card information, without stolen social security numbers, was sufficiently sensitive to give hackers the ability to commit fraud or identity theft, therefore establishing a substantial risk of harm.[151] Furthermore, the court indicated that, based on the Supreme Court's holding in *Clapper*, the certainly impending standard should be used in situations of national security, while the lower, substantial risk standard, should be used in all other cases.[152]

V. ANALYSIS

The Supreme Court has an opportunity to recognize the severity and immediacy of problems associated with data theft by allowing aggrieved parties to rightfully and litigate against companies that employ inadequate protections for consumers' sensitive personal information. The federal circuit courts use varying standards to evaluate whether data theft is sufficient to establish the injury-in-fact element of standing. The plaintiff-friendly *Remijas* court considered the intent of the hackers;[153] the plaintiff-friendly *Zappos* court looked at the sensitivity of the information;[154] the defendant-friendly *Beck* court considered the amount of time since a breach to determine whether a harm was speculative;[155] and finally, since *Clapper*, courts' opinions vary across the board regarding whether to use the certainly impending or the substantial risk standards, with some arguing that the certainly impending standard should only be used for instances implicating national security.[156]

The Supreme Court should resolve this circuit split by allowing consumers the ability to redress injuries resulting from the negligent or reckless conduct of companies. Accordingly, to resolve this federal circuit court split, the Supreme Court should use the next data breach case to establish the substantial risk standard as controlling in data breach litigation and require only a showing of a data breach resulting in the theft of sensitive information to establish constitutional standing. By resolving

---

[150] *Id.*
[151] *Id.* at 1029.
[152] *Id.* at 1026.
[153] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).
[154] *In re* Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018).
[155] Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017).
[156] *In re* Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018).

the circuit split, the Supreme Court can avoid problems associated with forum shopping, unintended injustices that prevent consumers from litigating their claims, confusion over which standard should be used to determine standing, and the specific requirements for establishing the injury-in-fact requirement of standing.

A. AN UNRESOLVED SPLIT AMONG THE FEDERAL CIRCUIT COURTS ENCOURAGES FORUM SHOPPING

The Supreme Court needs to resolve this circuit split to prevent forum shopping.[157] Currently, choice of forum may determine the result of cases alleging future harm due to data theft.[158] Companies are likely to take legal measures to ensure that they can litigate claims in defendant-friendly forums with defendant-friendly law, so as to make future litigation more predictable.[159] For instance, in their terms of service, they can insist on forum selection clauses,[160] choice of law clauses, or binding arbitration that would severely impact consumers ability to effectively fight for damages.[161] Defendants can also gain unfair advantages by forcing plaintiffs to litigate far from home in a forum that uses laws favorable to defendants.[162] Thus, a forum selection clause immediately leads to increased leverage in lawsuit negotiations.[163]

---

[157] "Forum Shopping" refers to a plaintiff choosing the court that will redress their injury most favorably, when multiple courts have concurrent jurisdiction. Forum Shopping, LEGAL INFO. INST., https://www.law.cornell.edu/wex/forum_shopping (last visited Sept. 2, 2021).

[158] Nancy R. Thomas, *No Injury, No Data Breach Claims? Depends on the Circuit*, MORRISON FOERSTER (Sept. 17, 2020), https://www.mofo.com/resources/insights/200917-no-data-breach-claims.html.

[159] *Keeping Current: U.S. Supreme Court Reaffirms that Forum-Selection Clauses Are Presumptively Enforceable*, AMERICAN BAR ASSOCIATION (Jan. 23, 2014), https://www.americanbar.org/groups/business_law/publications/blt/2014/01/keeping_current_duffee/.

[160] A forum selection clause specifies where the parties must litigate disputes arising under the contract. David C. McCormack. *Negotiating a Business Contract? Don't Ignore Forum Selection Clauses*, AXLEY ATTORNEYS (Dec. 10, 2020), https://www.axley.com/publication_article/forum-selection-clauses/.

[161] Jimmie E. Gates, *Arbitration Agreements: Hurting Consumers or Saving Money?*, CLARION LEDGER (May 5, 2017), https://www.clarionledger.com/story/news/2017/05/05/arbitration-agreements-hurting-consumers-saving-money/101284330/.

[162] *See Generally* James A. Meaney & Esra R. Jackson, *Forum Selection Clauses After Atlantic Marine*, AMERICAN BAR ASSOCIATION (Oct. 15-17, 2014), https://www.americanbar.org/content/dam/aba/events/franchising/materials2014/w4.pdf.

[163] David C. McCormack. *Negotiating a Business Contract? Don't Ignore Forum Selection Clauses*, AXLEY ATTORNEYS (Dec. 10, 2020), https://www.axley.com/publication_article/forum-selection-clauses/.

B. Relaxing the Standing Requirement Allows Consumers to Litigate Their Claims

Today, online purchases or applications commonly require the electronic dissemination of sensitive information, such as addresses, credit card numbers, and social security numbers.[164] As a result, consumers need to be able to hold negligent and reckless companies accountable for failing to adequately protect their sensitive information. Ten percent of Americans,[165] 33% of American adults, and 25% of adults at least 55 years old have experienced identity theft.[166] However, this is not only an adult problem.[167] One million children were victims of identity theft in 2017.[168] Identity theft is the most likely consequence of data breach, accounting for 65% of data breach incidents, which indicates a substantial risk of identity theft following data thefts.[169] Thus, the seriousness of data theft in America requires plaintiff-friendly enforcement standards that will hold companies accountable for maintaining strict safeguards.

To reiterate the *Remijas* court, granting a plaintiff standing to sue does not guarantee a favorable outcome on the merits.[170] Standing is merely a threshold matter.[171] However, if standing is not granted, victims of reckless and negligent data management by large companies and corporations would experience draconian effects.[172] The absence of a unified plaintiff-friendly standard preempts many Americans from any

---

[164] *See generally Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista (Jan. 12, 2021), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed.

[165] Sam Cook, *Identity Theft Facts & Statistics: 2019-2020*, Comparitech, https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/ (last updated Aug. 23, 2021).

[166] *Global Cybersecurity Awareness Survey Reveals 33 Percent of U.S. Respondents Have Experienced Identity Theft, More Than Twice the Global Average,* Proofpoint *(Oct. 11, 2018),* https://www.proofpoint.com/us/newsroom/press-releases/global-cybersecurity-awareness-survey-reveals-33-percent-us-respondents-have; Eugene Bekker*, What Are Your odds of Getting Your Identity Stolen?,* Identity Force *(Apr. 15, 2021),* https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.

[167] Kelli B. Grant, *Identity Theft Isn't Just an Adult Problem. Kids are Victims Too*, CNBC (Apr. 24, 2018, 9:23 AM), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html.

[168] Chris Morris, *More Than 1 Million Children Were Victims of Identity Theft in 2017*, Bus. Insider (Apr. 24, 2018, 12:45 PM), https://fortune.com/2018/04/24/stolen-identity-theft-children-kids/.

[169] Jennifer Bellemare, *What Are Your odds of Getting Your Identity Stolen?*, Identity Force (Oct. 28, 2020), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.

[170] *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 697 (7th Cir. 2015).

[171] Mendoza v. JPMorgan Chase Bank, N.A, 6 Cal.App.5th 802, 810.

[172] John A. Fisher, Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach, 4 WM. & Mary Bus. L. Rev. 215, 236 (2013), https://scholarship.law.wm.edu/wmblr/vol4/iss1/7.

redressability until they have already suffered the consequences of an injury, due to the difficulty of proving a future harm is certainly impending.[173]

The doctrine of standing has constitutional origins—a constitution that predates the invention of the internet. The Supreme Court should interpret the constitutional requirement of standing in a modern-day context so that American consumers can receive the justice and protection they deserve. Afterall, Americans experience identity theft at a rate twice the global average.[174]

C. ESTABLISHING THE SUBSTANTIAL RISK STANDARD AS CONTROLLING IN DATA THEFT CASES CAN RESOLVE THE FEDERAL CIRCUIT COURT SPLIT

Currently, lower courts have indicated that the substantial risk standard should be used in cases implicating national security.[175] Since *Clapper*, the federal circuit courts have shown a willingness to apply the less stringent, substantial risk standard to cases not involving questions of national security.[176] The substantial risk standard should be used in cases outside the national security context because the nature of future harms from data theft makes it significantly more difficult to prove that a harm is certainly impending.[177] Many data breaches result in the theft of a vast amount of personal information, making it difficult for plaintiffs to establish a certainty of future harm.[178] However, statistical research shows that actual injuries regularly follow from data thefts.[179] Policy should reflect support for injured parties who are susceptible to commonplace and life-altering harms that come from identity theft, rather than the defense of businesses and corporations that fail to adequately protect their customers' sensitive information.

---

[173] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401, 410 (2013).

[174] *Global Cybersecurity Awareness Survey Reveals 33 Percent of U.S. Respondents Have Experienced Identity Theft, More Than Twice the Global Average*, PROOF POINT (Oct. 11, 2018), https://www.proofpoint.com/us/newsroom/press-releases/global-cybersecurity-awareness-survey-reveals-33-percent-us-respondents-have.

[175] In re Zappos.com, Inc., 888 F.3d 1020, 1026 (9th Cir. 2018).

[176] *See Id.* at 1024-25.

[177] See Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy.").

[178] *See* Joseph Johnson, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, STATISTA (March 3, 2021), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[179] THE COUNCIL OF ECONOMIC ADVISORS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY (Feb. 2018). https://www.hsdl.org/?view&did=808776.

D. The Occurrence of a Data Theft of Sensitive Information Should be Sufficient to Establish the Injury-in-Fact Requirement

The courts have considered different kinds of information when determining whether a substantial risk of harm exists, including timing, intent, and sensitivity.[180] The risk of identity theft is fairly obvious today.[181] The impact of data thefts are no longer a mystery—over fifteen years of data supports the notion that data theft regularly occurs and its likelihood to result in injury.[182] For this reason, the only considerations into whether an injury-in-fact is established due to a future threat of harm should be (1) whether a data theft occurred, and (2) the sensitivity of the information.

An inquiry into the intent of a data theft should not be required because the occurrence of a data theft inherently indicates the intent to steal data and misappropriate its use.[183] Similarly, the amount of time elapsed since the occurrence of a data theft should not be relevant in determining an injury-in-fact. Once information is stolen, it can be passed around and sold for any extended period of time, resulting in a threat of identity risk that may never subside.[184] An approach that only looks at the sensitivity of the information and whether a data breach occurred would simplify the analyses for courts and relieve them from inquiring into redundant considerations. It would also provide the United States with a more simple, straightforward, and standardized way of dealing with questions of standing in threat of future harm, data theft cases.

Lastly, the sensitivity of the information should be the paramount inquiry into whether an injury-in-fact exists—only sensitive stolen data should confer standing on a plaintiff. Sensitive data includes personally identifiable information[185], personal health information[186], and financial

---

[180] *See supra* Analysis.

[181] *See Generally Global Cybersecurity Awareness Survey Reveals 33 Percent of U.S. Respondents Have Experienced Identity Theft, More Than Twice the Global Average*, Proof Point (Oct. 11, 2018), https://www.proofpoint.com/us/newsroom/press-releases/global-cybersecurity-awareness-survey-reveals-33-percent-us-respondents-have.

[182] *See* J. Charlton Collins, *Check on Data Breaches at the Privacy Rights Clearinghouse*, Journal of Accountancy (Sept. 1, 2019), https://www.journalofaccountancy.com/issues/2019/sep/data-breaches-privacy-rights-clearinghouse.html.

[183] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

[184] Adam Shell, *Equifax data breach could create lifelong identity theft threat*, USA Today (Sept. 9, 2021, 10:08 AM), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/.

[185] Personally identifiable information is "data that could be used to identify, contact, or locate a specific individual or distinguish one person from another: this information includes social security numbers, drivers' license numbers, addresses, and phone numbers." *Data Classification Guide*, Spirion (Last visited Nov. 3, 2021), https://www.spirion.com/data-classification/#phase-3.

information.[187] Plaintiffs should not be able to establish standing by alleging the disclosure or theft or other information that is publicly available, such as a telephone number or zip code. The injury must be supported by sensitive information that could result in more severe harms such as fraud or identity theft.

CONCLUSION

Data theft and data analytics are billion-dollar industries—and growing.[188] By stealing personal data, thieves cannot only commit identity fraud, but they can obtain much of the same information that businesses covet when marketing to consumers.[189] Customer data is an increasingly valuable commodity in itself,[190] and consumers need appropriate protection.

The Supreme Court can provide appropriate guidance by establishing a consistent standard that also provides consumers with a means of seeking redress for harms resulting from data theft. Companies that manage large quantities of consumer data have a duty to safeguard the information. By taking a more relaxed stance on establishing an injury-in-fact in cases alleging a future risk of injury, courts enable the public to fight back against negligent and reckless acts by people and businesses with whom they have entrusted their data. Currently, many companies are not held accountable for harmful business tactics,[191] in part because the Supreme Court has not given adequate guidance on the issue.

The Supreme Court should take advantage of the next data breach case to establish the more lenient substantial risk standard as the controlling standard in data breach cases. The Court should also require only an allegation of an actual data breach and theft of sensitive information to establish the injury-in-fact requirement. A consistent standard would al-

---

[186] Personal health information is health and medical information, including insurance, tests, and health status. *Data Classification Guide*, SPIRION (Last visited Nov. 3, 2021), https://www.spirion.com/data-classification/#phase-3.

[187] Financial information such as credit cards, bank account information, and passwords. *Data Classification Guide*, SPIRION (Last visited Nov. 3, 2021), https://www.spirion.com/data-classification/#phase-3.

[188] See *Big Data Analytics in Retail Market Expected to Reach $25.56 Billion by 2028,* ALLIED MRT. RSCH., https://www.alliedmarketresearch.com/press-release/big-data-analytics-in-retail-market.html (last visited Sept. 17, 2021).

[189] Rebeccah Jennings, *Why Targeted Ads are the Most Brutal Owns*, VOX (Sept. 25, 2018, 7:30 AM), https://www.vox.com/the-goods/2018/9/25/17887796/facebook-ad-targeted-algorithm.

[190] Leonard Murphy, *Personal Data: The Ultimate Commodity?*, GREENBOOK, (Sept. 21, 2017) https://www.greenbook.org/mr/market-research-news/personal-data-the-ultimate-commodity/.

[191] Sachin Gupta & Matthew J. Schneider, *Protecting Customers' Privacy Requires More than Anonymizing Their Data*, HARV. BUS. REV. (June 1, 2018), https://hbr.org/2018/06/protecting-customers-privacy-requires-more-than-anonymizing-their-data.

low consumers greater access to redressability and would also force businesses to act more responsibly with sensitive consumer data.