2021

Circuit Courts Split: Victim of a Data Breach? Can You “STAND” and Sue in Federal Court?

Darlyn de la Rosa

Florida International University College of Law, Ddela062@fiu.edu

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

Part of the [Communications Law Commons](#), [Consumer Protection Law Commons](#), and the [Internet Law Commons](#)

Online ISSN: 2643-7759

Recommended Citation

Darlyn de la Rosa, *Circuit Courts Split: Victim of a Data Breach? Can You “STAND” and Sue in Federal Court?*, 15 FIU L. Rev. 121 (2021).

DOI: <https://dx.doi.org/10.25148/lawrev.15.1.21>

This Comment is brought to you for free and open access by eCollections. It has been accepted for inclusion in FIU Law Review by an authorized editor of eCollections. For more information, please contact lisdavis@fiu.edu.

CIRCUIT COURTS SPLIT: VICTIM OF A DATA BREACH?
CAN YOU “STAND” AND SUE IN FEDERAL COURT?

Darlyn de la Rosa*

ABSTRACT

As data breaches become more frequent, those whose data has been stolen have begun to sue the companies that kept their personal data. In order to sue in federal court for this issue, the plaintiffs need to satisfy Article III standing. To satisfy Article III standing, plaintiffs need to show that they suffered an injury in fact. The Sixth, Seventh, Ninth, and D.C. Circuit Courts of Appeals have held that the risk of future identity theft arising from a data breach is enough to establish the injury requirement under Article III. Although not in a data breach case, the Eleventh Circuit has also found that the risk of identity theft is sufficient to establish an injury in fact. In contrast, the Second, Third, Fourth, and Eighth Circuit Courts of Appeals have refused to find an injury in fact based on the increased risk of identity theft arising from a data breach. Although not in a data breach case, the First Circuit Court of Appeals has also found that the risk of identity theft is not sufficient for a plaintiff to have standing to sue in federal court. The Fifth and Tenth Circuits have not yet weighed in on the issue. The Supreme Court has also refused its opportunity to address the circuit split. The Supreme Court should address the issue and find that a data breach victim has suffered an injury in fact based on an increased risk of identity theft because (1) previous Supreme Court decisions regarding an injury in fact support that finding; (2) statistics and legislative action show a correlation between data breaches and identity theft; and (3) finding an injury in fact is the equitable result based on the pervasiveness of data breaches and the burden a data breach imposes on a victim, including economic and emotional burden. The Court should find an injury in fact for all victims of a data breach, including victims of data breaches that occurred during a physical laptop or box theft, and when the information stolen in the breach is credit or debit card information.

I.	Introduction	123
II.	Background	126
	a. Types of Breaches and Statistics.....	126
	i. Data Breaches	126

* J.D. 2021, Florida International University College of Law.

	ii. Identity Theft.....	127
III.	Analysis.....	129
	a. Constitutional Standing Requirements.....	129
	i. Injury in Fact Requirement	131
	b. Circuit Split.....	133
	i. The Sixth, Seventh, Ninth, and D.C. Circuit Courts of Appeals Find that an Increased Risk of Future Identity Theft is Sufficient to Establish an Injury in Fact.	133
	ii. Although Not in a Data Breach Case, the Eleventh Circuit Has Found that the Risk of Identity Theft Is Sufficient for a Plaintiff to Have Standing to Sue in Federal Court.....	139
	iii. Notwithstanding the Strong Reasoning Presented by the Other Circuits, the Second, Third, Fourth, and Eighth Circuit Courts of Appeals Have Refused to Find an Injury in Fact Based on an Increased Risk of Identity Theft.	139
	iv. Although Not in a Data Breach Case, the First Circuit Court of Appeals Has Found that the Risk of Identity Theft Is Not Sufficient for a Plaintiff to Have Standing to Sue in Federal Court.	144
	v. The Fifth and the Tenth Circuit Courts of Appeals Have Not Analyzed Whether a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.	145
	vi. The Supreme Court Has Refused to Weigh in as to Whether Plaintiffs Who Sue in Federal Court and Claim an Increased Risk of Identity Theft Have Alleged an Injury in Fact.....	145
	c. Resolving the Circuit Split.....	146
	i. The Supreme Court's Previous Decisions that Relate Support a Finding that a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.	146
	ii. The Statistical Correlation Between Data Breaches and Identity Theft and Legislative Action Supports a Finding that a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.	149
	iii. Courts Should Find that Plaintiffs Who Have Been the Victims of a Data Breach Have Suffered an Injury in Fact Based on an Increased Risk of Identity Theft	

Because That Is an Equitable Result Based on the Pervasiveness of Data Breaches and the Burden a Data Breach Imposes on a Victim.....	150
1. Pervasiveness of Data Breaches	150
2. Mitigation Economic Costs of a Data Breach	151
3. Emotional Costs of a Data Breach.....	152
iv. Unlike the Fourth Circuit’s Finding in <i>Beck</i> , the Victim of a Data Breach from a Stolen Laptop Is Sufficient to Find that the Victim Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.....	152
v. Unlike the Eighth Circuit’s Decision in <i>Alleruzzo</i> , Stolen Credit Card Information Such as Credit Card Number, PIN, and Expiration Date Can Give Rise to an Injury in Fact Based on an Increased Risk of Identity Theft.	153
IV. Conclusion	154

I. INTRODUCTION

In this digital world we live in, everyone is at risk of becoming a victim of identity theft or some other data breach. With the rise of COVID-19,¹ the amount of people surfing the internet has increased, further exposing those working from home and using their computers to obtain information about the virus to data breaches and identity theft.² But the biggest question of all is, can we all sue?

---

¹ COVID-19 is a respiratory illness that can easily spread from person to person, leading people to practice social distancing, which includes working and attending schools remotely. *See* CENTERS FOR DISEASE CONTROL & PREVENTION, WHAT YOU NEED TO KNOW ABOUT CORONAVIRUS DISEASE 2019 (COVID-19), <https://www.cdc.gov/coronavirus/2019-ncov/downloads/2019-ncov-factsheet.pdf>.

² Preying on the public’s fear and need for information regarding COVID-19, hackers send emails claiming to be from legitimate organizations with information about the coronavirus with a link for statistical information. If the receiver opens the link, a malicious software will be installed on the receiver’s device and that device will allow cybercriminals to take control of the receiver’s computer, log their keystrokes, or access their personal information and financial data, which could lead to identity theft. *See* Steve Symanovich, *Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams*, NORTON (Mar. 5, 2020), <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>. *See* Dan Lohrmann, *How Is Covid-19 Creating Data Breaches?*, GOV’T TECH. (Mar. 30, 2020), <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-is-covid-19-creating-data-breaches.html> (“Most experts believe that public and private sector organizations will need to address numerous data breaches as a result of the extraordinary move to almost ubiquitous working from home within a few days and without much time for planning.”).

There are many examples of massive data breaches that have exposed billions of people's records around the world. For example, in 2013 and 2014, a data breach on Yahoo's database affected three billion user accounts and compromised the real names, email addresses, dates of birth, telephone numbers, and passwords of the users.³ The world's data volume has been continuing to grow significantly, giving cybercriminals a greater opportunity to steal massive volumes of data.⁴ With the rise of technology, unlimited access to the Internet for many, and the use of digital data, millions of people are affected yearly by data breaches.⁵ As a result, data breach occurrences have become a growing concern for many victims, who often seek relief in federal court for their increased risk of identity theft as a result of the data breach.⁶ Data breach victims often sue the company that had access to the victim's data for mishandling the data and allowing cybercriminals to get their hands on it.⁷

Based on the rising nature of data breaches, federal courts have been asked on multiple occasions to determine whether plaintiffs who have been victims of data breaches can establish Article III standing based on an increased risk of future identity theft stemming from a data breach.⁸ Specifically, these courts have been asked to determine whether the plaintiffs have suffered an injury in fact, sufficient to establish Article III standing in a federal court.⁹ The federal circuits are sharply divided over this issue.¹⁰ On one hand, the Sixth, Seventh, Ninth, and D.C. Circuit Courts of Appeals have held that the risk of identity theft is sufficient to establish an injury in fact because the primary reason to execute a data breach is to steal the victim's identity, and therefore, a substantial risk of identity theft exists.¹¹ The

---

³ Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Jan. 8, 2021), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

⁴ Juliana De Groot, *The History of Data Breaches*, DATA INSIDER DIGITAL GUARDIAN'S BLOG (Dec. 1, 2020), <https://digitalguardian.com/blog/history-data-breaches>.

⁵ *Id.*; Robert Siciliano, *Identity Theft Crimes by the Numbers*, BALANCE (Dec. 5, 2019), <https://www.thebalance.com/identity-theft-crimes-by-the-numbers-4157714>.

⁶ Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, A.B.A. (July 17, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2018/07/data-breach/.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ See *In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018); *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 Fed. Appx. 384 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015); *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, 928 F.3d 42 (D.C. Cir. 2019); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

Eleventh Circuit has not specifically addressed an increased risk of identity theft based on a data breach but it has found that a plaintiff has suffered an injury in fact based on an increased risk of identity theft under other circumstances.¹² In contrast, the Second, Third, Fourth, and Eighth Circuit Courts of Appeals have found that victims of data breaches have not suffered an injury in fact based on an increased risk of future identity theft because the alleged injury is too speculative.¹³ Although not specifically addressing the risk of identity theft stemming from a data breach, the First Circuit has also found that an increased risk of identity theft is not sufficient to establish an injury in fact.¹⁴ The Fifth and Tenth Circuits have not yet weighed in on the issue.¹⁵

This article will address that based on the principle that victims of a data breach suffer a “substantial risk” of future identity theft, these victims can prove an injury in fact sufficient for Article III standing because Supreme Court decisions, statistics, and legislative action support that finding. First, this article will provide definitions and background statistics on data breaches and identity theft. Second, this article will describe the elements of standing and under what circumstances the Supreme Court has found that a plaintiff has suffered an injury in fact. Next, this article will analyze the current circuit split on this issue, under what factual scenarios the circuit splits arise, how the courts have reached their decisions, and the reasoning behind each decision. Finally, this article will explain the Supreme Court’s current stance on the issue and why plaintiffs who have been the victims of a data breach have suffered an injury in fact based on an increased risk of identity theft.

---

¹² Christopher P. Hahn, *11 Cir. Splits from Other Circuits on Spokeo Standing*, MAURICEWUTSCHER THE CONSUMER FIN. SERV. BLOG (May 16, 2019), <https://consumerfsblog.com/2019/05/11th-cir-splits-from-other-circuits-on-spokeo-standing/>.

¹³ *Alleruzzo v. SuperValu, Inc.* (*In re SuperValu, Inc., Customer Data Sec. Breach Litig.*), 870 F.3d 763 (8th Cir. 2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011).

¹⁴ *Katz v. Pershing, LLC*, 672 F.3d 64, 77 (1st Cir. 2012).

¹⁵ Allison Grande, *DC Cir. Piles onto Standing Split with Data Breach Ruling*, LAW360 (June 28, 2019), <https://www.law360.com/articles/1173454/dc-circ-piles-onto-standing-split-with-data-breach-ruling>.

II. BACKGROUND

a. Types of Breaches and Statistics

i. Data Breaches

Data breaches take place when a customer's personal information becomes exposed to internet predators.¹⁶ Specifically, a data breach takes place when cyber hackers gain unauthorized access to a corporation's database.¹⁷ In these corporate databases, the cyber hackers usually find customer data such as passwords, credit card numbers, Social Security numbers, banking information, driver's license numbers, medical records, and other sensitive information.¹⁸ The purpose of hacking these systems is to use this information for identity theft and fraud.¹⁹ Data breaches can take place by physically accessing a computer or network to steal local files or by bypassing network security remotely.²⁰

Data breaches have affected the companies' databases that most Americans use frequently, and new breaches occur daily. For example, in March 2020, Princess Cruises admitted that it was the victim of a data breach.²¹ Possible data accessed included names, addresses, Social Security numbers, and government IDs, along with financial and health information of its customers.²² In addition, from 2014 to 2018, cyber thieves stole information from 500 million customers of Marriot International, including some combination of contact information, passport numbers, Starwood Preferred Guest numbers, travel information, credit card numbers, and credit card expiration dates.²³ In May of 2014, a cyberattack exposed the information of all of eBay's 145 million users, including the names, addresses, dates of birth, and encrypted passwords of all these users.²⁴ In 2007, TK/TJ Maxx suffered a data breach where more than 94 million records

---

¹⁶ Steve Symanovich, *What Is a Data Breach and How Do I Handle One?*, LIFELOCK (July 31, 2017), <https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html>.

¹⁷ Nicole Martin, *What Is a Data Breach*, FORBES (Feb. 25, 2019), <https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#66e350d14bbe>.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ *Id.*

²¹ Zack Whittaker, *Princess Cruises, Hobbled by the Coronavirus, Admits Data Breach*, TECH CRUNCH (Mar. 13, 2020), <https://techcrunch.com/2020/03/13/princess-cruises-coronavirus-breach/>.

²² *Id.*

²³ Swinhoe, *supra* note 3.

²⁴ *Id.*

were compromised.²⁵ In 2010, Sony PlayStation Network suffered a data breach where 77 million records were compromised.²⁶ In 2013, Target’s server was compromised and 70 million records were stolen.²⁷ In 2014, JP Morgan suffered a data breach and 56 million records were compromised.²⁸ Similarly, Chase’s database was compromised in 2014 and 76 million records were stolen.²⁹ In July of 2019, a data breach to Capital One Financial Corporation exposed 100 million records.³⁰

In addition, statistics of data breaches show an exponential increase in the number of data breaches or the number of records affected reported since 2013.³¹ For example, in 2013, 614 company data breaches were reported, resulting in 91.98 million records stolen.³² In 2014, 783 data breaches were reported, resulting in 85.61 million records stolen.³³ In 2016, 1,093 data breaches took place in the United States, and that number increased to 1,579 data breaches in 2017.³⁴ In 2017, 197.61 million records were exposed.³⁵ While 1,244 data breaches took place in the United States in 2018, more than 446.5 million records were exposed, which is the highest number of exposed records since 2005.³⁶ In 2019, there were 1,437 breaches, up seventeen percent from 2018 but below the number of breaches in 2017.³⁷

ii. Identity Theft

Identity theft takes place after a data breach when cybercriminals use stolen customer data to make purchases, apply for loans, withdraw money,

---

²⁵ De Groot, *supra* note 4.

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last visited Feb. 25, 2020) [hereinafter INSURANCE INFORMATION INSTITUTE].

³¹ De Groot, *supra* note 4.

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ 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/>.

³⁶ *Id.*; Ben Luthi, *What Is Identity Theft*, EXPERIAN (Oct. 7, 2019), <https://www.experian.com/blogs/ask-experian/what-is-identity-theft/>.

³⁷ INSURANCE INFORMATION INSTITUTE, *supra* note 30.

or commit fraud.³⁸ Identity theft is the fastest growing crime in America, impacting more than 16.7 million Americans in 2017.³⁹ In 2018, although the number of identity theft victims was 14.4 million, 3.3 million people were responsible for some financial liability of the fraud committed against them.⁴⁰ In 2018, identity theft victims bore \$1.7 billion in out-of-pocket identity theft costs.⁴¹

Identity theft has severe consequences for children and adults. For example, in 2017, one million of the identity theft victims were children, causing the families more than \$540 million in out of pocket expenses and a total of \$2.6 billion in losses.⁴² Statistics also show that 77.3 percent of identity theft victims report emotional distress stemming from identity theft.⁴³ Among those victims, children also experience emotional distress, such as stress, anger, and concern by the theft of their personal information.⁴⁴ In general, identity theft victims suffer financial stress and exhibit similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility.⁴⁵ Victims also often experience loss of confidence in areas where they typically had confidence, sleeplessness, isolation, self-blame, vulnerability, difficulty eating, self-medication with alcohol or food, and loss of motivation.⁴⁶ When it comes to family relations, identity theft can also cause trouble at home, with 17 percent of victims reporting suffering in their personal relationships as a result of the child identity fraud.⁴⁷ These identity theft instances lead parents to believe that they should have done more to protect their children from identity theft, and the child victims also feel the same way.⁴⁸

---

³⁸ *What to Know About Identify Theft*, FEDERAL TRADE COMMISSION, <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited Apr. 19, 2021).

³⁹ Bill Fay, *What Is Identity Theft?*, DEBT.ORG (May 22, 2020), <https://www.debt.org/credit/identity-theft/>.

⁴⁰ INSURANCE INFORMATION INSTITUTE, *supra* note 30.

⁴¹ *Id.*

⁴² Jennifer Bellemare, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Oct. 28, 2020), <https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics>; Stefan Lembo Stolba, *The Emotional Toll of Child Identity Theft*, EXPERIAN (Aug. 29, 2018), <https://www.experian.com/blogs/ask-experian/the-emotional-toll-of-child-identity-theft/>.

⁴³ Bellemare, *supra* note 42.

⁴⁴ Stolba, *supra* note 42.

⁴⁵ EQUIFAX, A LASTING IMPACT: THE EMOTIONAL TOLL OF IDENTITY THEFT (Feb. 2015), https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

⁴⁶ *Id.*

⁴⁷ Stolba, *supra* note 42.

⁴⁸ *Id.*

In addition, identity theft is one of the most common consequences of data breaches.⁴⁹ For example, in 2016, 31.7 percent of breach victims later experienced identity theft, compared to just 2.8 percent of individuals not notified of a data breach in 2016.⁵⁰ Worldwide, identity theft is the most common type of data breach incident, accounting for 59 percent of all global data breach incidents in 2016.⁵¹ Regardless, whether the breach is a data breach or identity theft, the victims should have a right to bring an action in federal court. The next section addresses the requirements the victim must meet to bring such an action in federal court and the current stance of the district courts on this issue.

III. ANALYSIS

a. Constitutional Standing Requirements

Under Article III of the Constitution, the jurisdiction of federal courts is limited to *Cases* and *Controversies*.⁵² In *Raines*, the Supreme Court explained that “[n]o principle is more fundamental to the judiciary’s proper role in our system of government than the constitutional limitation of federal court jurisdiction to actual cases or controversies.”⁵³ In other words, this restriction is critical to the success of our separation of powers structure.⁵⁴ To satisfy this constitutional requirement, a plaintiff must have *standing* to sue.⁵⁵ “[T]he question of standing is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.”⁵⁶

At an irreducible constitutional minimum, standing requires the plaintiff to prove three elements.⁵⁷ First, the plaintiff must have suffered an “injury in fact,” which is an invasion of a legally protected interest that is concrete and particularized, and “actual or imminent, not ‘conjectural’ or

---

⁴⁹ Bellemare, *supra* note 42.

⁵⁰ Matt Tatham, *Identity Theft Statistics*, EXPERIAN (Mar. 15, 2018), <https://www.experian.com/blogs/ask-experian/identity-theft-statistics/>.

⁵¹ *Gemalto Releases Findings of 2016 Breach Level Index*, THALES GROUP (Mar. 28, 2017), <https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/gemalto-releases-findings-of-2016-breach-level-index#:~:text=Identity%20theft%20was%20the%20leading,the%20time%20they%20were%20reported.>

⁵² *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 559 (1992).

⁵³ *Raines v. Byrd*, 521 U.S. 811, 818 (1997).

⁵⁴ *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006).

⁵⁵ *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 408 (2013).

⁵⁶ *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004).

⁵⁷ *Lujan*, 504 U.S. at 560.

‘hypothetical.’”⁵⁸ The injury in fact requirement of standing “serves to ensure that the plaintiff has a personal stake in the litigation.”⁵⁹ For example, in *Monsanto*, the Court found that a group of conventional alfalfa growers had suffered an injury in fact as a result of a government decision to deregulate genetically engineered alfalfa.⁶⁰ Specifically, the conventional growers alleged that the deregulation would harm them because their neighbors would plant genetically engineered seeds, bees would obtain pollen from those plants, and the bees would then contaminate the farmers’ own conventional alfalfa with the genetically modified gene.⁶¹ The Court held that the conventional growers suffered an injury in fact because they would have to conduct testing to find out whether and to what extent their crops have been contaminated, and they would have to take measures to minimize the likelihood of potential contamination and to ensure an adequate supply of non-genetically-engineered alfalfa.⁶² The Court found that there was an injury in fact even when the crops were not infected with the genetically modified gene.⁶³

Second, the plaintiff must show a causal connection between the injury and the conduct complained of.⁶⁴ To meet the causal connection element, the injury must be “fairly . . . traceable to the challenged action of the defendant, and not . . . the result [of] the independent action of some third party not before the court.”⁶⁵ For example, in *Duke Power*, the Court found a causal connection between passing a law that limited the liability of private utilities in the event of nuclear accidents and provided for indemnification, and the environmental and aesthetic harm alleged by plaintiffs because “but for” the passage of the law there was a “substantial likelihood” that the nuclear power plants would not be constructed, and therefore the environmental and aesthetic harm alleged by plaintiffs would not occur.⁶⁶

Third, it must be “likely,” as opposed to merely “speculative,” that the injury will be “redressed by a favorable judicial decision.”⁶⁷ For example, in *Simon*, the Court held that poor people who had been denied service at certain hospitals failed to meet the redressability element because the poor

---

⁵⁸ *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

⁵⁹ *Attias v. CareFirst, Inc.*, 865 F.3d 620, 626 (D.C. Cir. 2017).

⁶⁰ *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 153–56 (2010).

⁶¹ *Id.*

⁶² *Id.* at 154.

⁶³ *Id.* at 155.

⁶⁴ *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

⁶⁵ *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992).

⁶⁶ *Duke Power Co. v. Carolina Env'tl. Study Grp.*, 438 U.S. 59, 72–78 (1978).

⁶⁷ *Spokeo*, 136 S. Ct. at 1547.

individuals could not show that changing the challenged IRS policy (extended tax benefits to hospitals that did not serve indigents) would cause the hospitals to alter their policies and treat them.⁶⁸

i. Injury in Fact Requirement

A plaintiff can establish an injury in fact by claiming a future injury when that injury is (a) “certainly impending” or (b) if there is a “substantial risk” that the harm will occur.⁶⁹ For example, in the landmark case *Lujan*, environmental organizations dedicated to the protection of wildlife sued the government for new regulations that limited the geographic scope of previous environmental regulations.⁷⁰ The previous environmental regulations required federal agencies to consult with the Secretary of the Interior or the Secretary of Commerce before undertaking actions that could jeopardize endangered or threatened species, which extended to actions taken in foreign nations.⁷¹ The purpose of the environmental regulations was to protect the continued existence of any endangered species or threatened species and to prevent the destruction or adverse modification of the habitats of such species.⁷² The organizations claimed to have standing based on some of the members’ testimony that they had traveled to different countries to observe endangered species and planned to travel to those countries again in the future.⁷³ For example, one of the members of one of the environmental organizations claimed that she traveled to Egypt in 1986 to observe the traditional habitat of the endangered Nile crocodile and she intended to do so again.⁷⁴ Another member claimed that she traveled to Sri Lanka in 1981 and observed the habitat of the Asian elephant and leopard, both endangered species, and that she intended to return to Sri Lanka in the future to observe the elephant and leopard since she had not been able to spot them in her previous trip.⁷⁵ The Court rejected the organizations’ theory of standing because it was based on the organizations’ members’ intent to return to these locations someday, and it was not “imminent.”⁷⁶

---

⁶⁸ *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 46 (1976).

⁶⁹ *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 168 (2014); *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013).

⁷⁰ *Lujan*, 504 U.S. at 558–59.

⁷¹ *Id.*

⁷² *Id.* at 558.

⁷³ *Id.* at 563–64.

⁷⁴ *Id.* at 563.

⁷⁵ *Id.*

⁷⁶ *Id.* at 564 n.2.

Similarly, in *Clapper*, where the Court also held that an injury was not imminent, attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive privileged communications with individuals abroad challenged a provision of the Foreign Intelligence Surveillance Act.⁷⁷ The challengers argued that “objectively reasonable likelihood” that their private conversations with foreigners would be intercepted.⁷⁸ The challengers claimed that they communicate “with people the Government ‘believes or believed to be associated with terrorist organizations,’ ‘people located in geographic areas that are a special focus’ of the Government’s counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government.”⁷⁹ The Court held that the attorneys and human rights, labor, legal, and media organizations had not suffered an injury in fact because that injury rested on a “highly attenuated chain of possibilities” and therefore, the injury was too speculative to satisfy the injury in fact requirement.⁸⁰ Specifically, the U.S. persons had to rely on a series of possibilities, such as whether intelligence officials would seek to use the surveillance methods under the challenged provision or whether judges would authorize such surveillance.⁸¹

Similarly, in *Lyons*, where the Court found that the Plaintiff had not suffered an injury in fact, a man was stopped by four police officers of the City of Los Angeles for a traffic or vehicle code violation.⁸² Although the man offered no resistance or threat, the officers seized the man and applied a chokehold technique, either a “bar arm control” or the “carotid-artery control” or both, and rendered the man unconscious and caused damage to his larynx.⁸³ The man alleged that the police from the City of Los Angeles regularly and routinely applied these chokeholds when they are not threatened by the use of any deadly force.⁸⁴ The Court held that in this civil rights action, the man lacked standing to enjoin the Los Angeles Police Department from using the controversial chokehold techniques on arrestees.⁸⁵ The Court held that although the arrestee had already been subjected to this treatment, which rendered him unconscious, the future harm

---

⁷⁷ *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 404–06, 410 (2013).

⁷⁸ *Id.* at 410.

⁷⁹ *Id.* at 406.

⁸⁰ *Id.* at 410.

⁸¹ *Id.* at 413.

⁸² *City of Los Angeles v. Lyons*, 461 U.S. 95, 98 (1983).

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.* at 105–06.

he sought to enjoin depended on the police arresting him and choking him again.⁸⁶ The Court found that this injury was too speculative.⁸⁷

In contrast, in *Driehaus*, the Court found an injury in fact where a former Congressman filed a complaint with the Ohio Elections Commission and claimed that an advocacy group violated an Ohio law that criminalizes false statements made during a political campaign.⁸⁸ The advocacy group made a statement saying that the Congressman’s vote in favor of the Affordable Care Act was a vote in favor of taxpayer-funded abortion.⁸⁹ After the Congressman lost the election, the Congressman dismissed the complaint, but the advocacy group sued in federal court challenging the Ohio law on First Amendment grounds.⁹⁰ The Court held that the advocacy group had standing to bring a pre-enforcement challenge to an Ohio statute prohibiting false statements during election campaigns.⁹¹ The Court reasoned that the advocacy group had suffered an injury in fact because the group could face criminal prosecution, it faced a substantial risk of administrative enforcement based on the history of past enforcement, and because any person with knowledge of the purported violation could file a complaint against the group.⁹² The Court found an injury in fact even though the challenge was based on a complaint that had not been made regarding a statement the group had not yet uttered against a candidate not yet identified.⁹³ The Federal Circuits are split in their decisions as to what is sufficient to establish an injury in fact.

b. Circuit Split

- i. The Sixth, Seventh, Ninth, and D.C. Circuit Courts of Appeals Find that an Increased Risk of Future Identity Theft is Sufficient to Establish an Injury in Fact.

Courts in the Sixth, Seventh, Ninth, and DC Circuits have been adamant in providing data breach victims with the opportunity to seek relief for their heightened risk of identity theft and inconveniences that arise as a result of

---

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 151–52 (2014).

⁸⁹ *Id.* at 153–54.

⁹⁰ *Id.* at 154–55.

⁹¹ *Id.* at 161.

⁹² *Id.*

⁹³ *Id.* at 160–65.

the breach. The following paragraphs provide a summary of these circuits' stance and how they have arrived at their decisions.

Precedent from the Sixth Circuit Court of Appeals establishes that a plaintiff's increased risk of identity theft after a data breach is sufficient to prove an injury in fact.⁹⁴ For example, in *Galaria*, cyber hackers broke into an insurance and financial services company's database that maintained records containing customers' sensitive personal information such as names, dates of birth, marital statuses, genders, occupations, employers, Social Security numbers, and driver's license numbers.⁹⁵ The court found that the customers met the injury requirement because they alleged a substantial risk of harm for suffering future identity theft and for reasonably incurring mitigation costs to deal with the effects of having personal data stolen.⁹⁶ The court reasoned that when a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victim's data for fraudulent purposes.⁹⁷ The court highlighted that although it might not be "literally certain" that a data breach victim's data will be misused, there is a sufficiently substantial risk of harm that victims will incur mitigation costs.⁹⁸ The court further explained that where customers already know that they lost control of their data, it would be unreasonable to expect the customers to wait for actual identity theft or fraud to occur before taking steps to ensure their personal and financial security, and file suit against the company for its negligence in handling the data.⁹⁹

The Seventh Circuit Court of Appeals also found in several cases that plaintiffs who were victims of data breaches suffered an injury in fact necessary to establish standing based on an increased risk of identity theft.¹⁰⁰ For example, in *Remijas*, Neiman Marcus customers sued the high-end department store because the store suffered a data breach that potentially exposed the customers' credit card information.¹⁰¹ The customers alleged that they had standing to sue based on the increased risk of future fraudulent charges and greater susceptibility to identity theft.¹⁰² The Seventh Circuit held that the customers' increased risk of identity theft was concrete and

---

⁹⁴ *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016).

⁹⁵ *Id.* at 386.

⁹⁶ *Id.* at 388.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 697 (7th Cir. 2015); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 970 (7th Cir. 2016).

¹⁰¹ *Remijas*, 794 F.3d at 690.

¹⁰² *Id.* at 692.

particularized enough to support Article III standing.¹⁰³ The court found that the increased risk of identity theft was not a mere allegation of possible future injury but the type of “certainly impending” future harm that the Supreme Court requires to establish standing.¹⁰⁴ The court reasoned that the alleged data breach had already occurred—stealing all the customers’ personal data—and therefore the court did not need to speculate as to whether the information had been stolen or what kind of information had been stolen.¹⁰⁵ The court further explained that the customers should not have to wait until the hackers committed identity theft to give them standing because there was an “objectively reasonable likelihood” that such injury would occur.¹⁰⁶

In addition, in *Remijas*, the court also noted that requiring the customers to wait until their identity was actually stolen would make it more difficult for the customers to meet the “fairly traceable” element of standing.¹⁰⁷ Specifically, the court reasoned that “the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not ‘fairly traceable’ to the defendant’s data breach.”¹⁰⁸ The court also noted that the only reason hackers would break into the store’s database and steal consumers’ private information is to sooner or later assume the customers’ identities.¹⁰⁹

Similarly, in *Lewert*, the court found the increased risk of identity theft was concrete where restaurant customers sued P.F. Chang’s alleging increased risk of identity theft based on a data breach that exposed consumer credit and debit card data.¹¹⁰ After the data breach, one of the named customers for this class action purchased a credit monitoring service to protect against identity theft, including against criminals using the stolen card’s data to open new credit or debit cards in his name.¹¹¹ Although the other named customer did not spot any fraudulent charges on his card, nor did he cancel his card or suffer the associated inconvenience or costs, he did spend time and effort monitoring his card statements and his credit report to ensure that no fraudulent charges had been made on his card or that no fraudulent accounts had been opened in his name.¹¹² The Seventh Circuit held

---

¹⁰³ *Id.* at 693.

¹⁰⁴ *Id.* at 692.

¹⁰⁵ *Id.* at 693.

¹⁰⁶ *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

¹⁰⁷ *Id.*

¹⁰⁸ *Id.* (quoting *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 2014 (N.D. Cal. 2014)).

¹⁰⁹ *Id.*

¹¹⁰ *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 965 (7th Cir. 2016).

¹¹¹ *Id.*

¹¹² *Id.*

that the increased risk of identity theft was concrete enough to support a lawsuit.¹¹³ The court reasoned that a substantial risk of harm arose from the data breach because the primary incentive for hackers is to assume those consumers' identities or to make fraudulent charges to their credit cards.¹¹⁴ The court explained that even though some of the customers could have canceled their credit cards, they all still faced the risk of identity theft, and that was sufficient to establish the injury in fact element of standing.¹¹⁵

Similar to the Sixth and Seventh Circuits, the Ninth Circuit has also found that plaintiffs can meet the injury in fact element by claiming increased risk of identity theft stemming from a data breach.¹¹⁶ For example, in *Krottner*, former and current employees sued Starbucks because their names, addresses, and Social Security numbers were stored on a laptop that a thief stole from Starbucks.¹¹⁷ The Ninth Circuit held that the employees' increased risk of future identity theft was sufficient to establish an injury in fact because the employees faced a "credible threat of harm," that was both "real and immediate" and not "conjectural or hypothetical."¹¹⁸ The court further explained that the employee's allegations were more than "conjectural or hypothetical" because the laptop containing the customer's unencrypted personal information had already been stolen.¹¹⁹ The court clarified that it would not have reached the same decision if the employees had sued when the laptop had not been stolen and the customers would have claimed an injury in fact based on the risk that the laptop would have been stolen at some point in the future.¹²⁰

Similarly, in *In re Zappos.com*, a Ninth Circuit case, the court found an injury in fact where customers sued online retailer Zappos after hackers breached Zappos' database and allegedly stole personal identifying information belonging to 24 million customers, including their "names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information."¹²¹ The customers claimed that they met the injury in fact requirement of standing

---

¹¹³ *Id.* at 967.

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ *In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018); *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).

¹¹⁷ *Krottner*, 628 F.3d at 1140.

¹¹⁸ *Id.* at 1143.

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *In re Zappos.com, Inc.*, 884 F.3d at 894–95.

because the Zappos data breach put them at risk of identity theft.¹²² In this case, the customers relied on the United States Government Accountability Office for the definition of identity theft, which includes “various types of criminal activities, such as when Personal Identifying Information is used to commit fraud or other crimes,” including “credit card fraud, phone or utility fraud, bank fraud, and government fraud.”¹²³ The court held that the customers had alleged an injury in fact sufficient to establish standing because the information stolen, which included credit card numbers, could be easily used to commit identity theft.¹²⁴ In addition, the court noted that even if a long time had passed between the breach and the customers’ suit, the customers’ injury was imminent because “a person whose personal identifying information has been obtained and compromised may not see the full extent of identity theft or identity fraud for years.”¹²⁵

The Circuit Court of Appeals for the District of Columbia has also held that the increased risk of identity theft arising from a data breach is sufficient to establish an injury in fact for standing purposes.¹²⁶ For example, in *Attias*, the customers of a health insurance company sued the insurance company for a cyberattack that exposed the customer’s personal identifying information such as their credit card numbers and Social Security numbers.¹²⁷ The court found that the customers met their burden of proving an injury in fact because the customers’ heightened risk of identity theft was substantial enough.¹²⁸ The court reasoned that the breach “exposed all of the information wrongdoers need” to steal a victim’s identity.¹²⁹ In addition, the court reasoned that the hackers had already gained access to the unauthorized information, and it was reasonable to infer that the hackers had the intent and ability to use the data for “ill.”¹³⁰ The court also stated that the hackers’ purpose in breaking into a database and stealing consumers’ private information is to make fraudulent charges or assume those consumers’ identities.¹³¹ The court explained that a substantial risk of harm existed simply by virtue of the hack and the nature of the data that the customers

---

¹²² *Id.* at 894.

¹²³ *Id.* at 895.

¹²⁴ *Id.*

¹²⁵ *Id.* at 900.

¹²⁶ *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, 928 F.3d 42 (D.C. Cir. 2019); *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

¹²⁷ *Attias*, 865 F.3d at 622, 628.

¹²⁸ *Id.*

¹²⁹ *Id.*

¹³⁰ *Id.* at 628.

¹³¹ *Id.* at 628–29.

alleged was taken.¹³² The court noted that the customers did not need to rely on a series of “uncertain contingencies involving multiple independent actors” before the customers suffered any harm.¹³³

Similarly, in *OPM*, another D.C. Circuit case, the court found an injury in fact where cyber attackers breached U.S. government employee databases and stole government employees’ sensitive personal information, including birth dates, Social Security numbers, addresses, and fingerprint records.¹³⁴ The court held that the government employees established the injury in fact element because they faced a “substantial” risk of future identity theft.¹³⁵ First, the court reasoned that the hackers had in their possession all the information they needed to steal the employees’ identities, including the employees’ social security numbers, birth dates, and addresses.¹³⁶ Second, the court noted that the employees’ faced a substantial risk of identity theft because sensitive personal information cannot be changed to avoid identity theft.¹³⁷ For example, while existing credit card numbers can be changed to prevent future fraud, Social Security numbers and addresses cannot be easily changed for new ones, and “birth dates and fingerprints stay with us forever.”¹³⁸ Third, the court highlighted that the employees’ risk of identity theft was substantial because some of the employees had already experienced various types of identity theft, such as the unauthorized opening of new credit cards and the filing of fraudulent tax returns in their names.¹³⁹ Lastly, the court reasoned that the attackers had intentionally targeted stealing the employees’ private information.¹⁴⁰

While several federal courts such as the Sixth, Seventh, Ninth, and D.C. Circuits have expressly ruled on this standing issue in regard to data breaches, some courts like the Eleventh Circuit have however, issued opinions on risks of identity theft standing that would also allow victims to bring such cases in Federal court.

---

¹³² *Id.*

¹³³ *Id.* at 628–29.

¹³⁴ *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, 928 F.3d 42, 49 (D.C. Cir. 2019).

¹³⁵ *Id.* at 56.

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.* at 58.

- ii. Although Not in a Data Breach Case, the Eleventh Circuit Has Found that the Risk of Identity Theft Is Sufficient for a Plaintiff to Have Standing to Sue in Federal Court.

Although the Eleventh Circuit has not issued an opinion regarding an increased risk of identity theft resulting from a data breach, the Eleventh Circuit has found standing in an increased risk of identity theft under other circumstances.¹⁴¹ For example, in *Muransky*, the Eleventh Circuit found that a consumer had suffered an injury in fact when Godiva issued him a receipt that showed his credit card number’s first six and last four digits in violation of the Fair and Accurate Credit Transactions Act (“FACTA”).¹⁴² In that case, the Eleventh Circuit found an injury in fact based on the customer’s heightened risk of identity theft stemming from Godiva’s violation of FACTA.¹⁴³ The court noted that the customer had established risk of real harm to a concrete interest sufficient to establish standing because a consumer undoubtedly has a concrete interest in preventing his identity from actually being stolen.¹⁴⁴

- iii. Notwithstanding the Strong Reasoning Presented by the Other Circuits, the Second, Third, Fourth, and Eighth Circuit Courts of Appeals Have Refused to Find an Injury in Fact Based on an Increased Risk of Identity Theft.

Presented with the opportunity to redress the inconveniences of millions of individuals whose personal information is stolen yearly through data breaches as a result of companies’ mishandling their data, the Second, Third, Fourth, and Eighth Circuit Courts of Appeals have refused to find that these individuals have suffered an injury in fact.¹⁴⁵ For example, the Second Circuit Court of Appeals has found that under certain circumstances, an increased risk of identity theft arising from a data breach is not sufficient to establish the injury in fact requirement for standing.¹⁴⁶ For example, in

---

¹⁴¹ Hahn, *supra* note 12.

¹⁴² *Id.*

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ See *Whalen v. Michaels Stores, Inc.*, 689 F. App’x 89, 91 (2d Cir. 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011); *Beck v. McDonald*, 848 F.3d 262, 277–78 (4th Cir. 2017); *Alleruzzo v. SuperValu, Inc. (In re SuperValu, Inc., Customer Data Sec. Breach Litig.)*, 870 F.3d 763, 770 (8th Cir. 2017).

¹⁴⁶ *Whalen*, 689 F. App’x at 91.

Whalen, Michaels, the arts and crafts store, suffered a data breach.¹⁴⁷ A customer sued Michaels after receiving two fraudulent charges on the same credit card she had used to shop at Michaels.¹⁴⁸ The customer alleged that her credit card was physically presented for payment to a gym in Ecuador for a charge of \$398.16.¹⁴⁹ The credit card was also presented for payment to a concert ticket company in Ecuador for a value of \$1,320.00.¹⁵⁰ Among her theories of injuries, the customer asserted an increased risk of future identity theft.¹⁵¹ The court held that the customer did not allege a concrete and particularized injury because she failed to show how she could “plausibly face a threat of future fraud.”¹⁵² The court reasoned that the customer had canceled her credit card after the breach and that no other personally identifying information, such as name, address, PIN, social security, or date of birth, had been stolen in the breach.¹⁵³ In this case, no charges were actually incurred on the card and she was not liable for any of the attempted charges.¹⁵⁴ In addition, the court reasoned that the customer lacked standing because she failed to allege with any specificity if she had spent any time or money monitoring her credit.¹⁵⁵

The Third Circuit Court of Appeals has also found that an increased risk of identity theft is not sufficient to establish Article III standing.¹⁵⁶ For example, in *Reilly*, cyber hackers infiltrated a payroll processor’s network and “potentially gained access to personal and financial information” belonging to employees.¹⁵⁷ The personal information obtained included the employees’ names, addresses, Social Security numbers, dates of birth, and bank account information.¹⁵⁸ This case was decided before *Clapper*, where the Supreme Court elicited the “substantial risk test.”¹⁵⁹ In *Reilly*, the Third Circuit held that the employees had not established an injury in fact based on an increased risk of future identity theft because the identity theft was not

---

¹⁴⁷ *Id.* at 90.

¹⁴⁸ *Id.*

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ *Id.* at 90.

¹⁵² *Id.*

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011).

¹⁵⁷ *Id.* at 40.

¹⁵⁸ *Id.*

¹⁵⁹ *Id.* at 40, 42.

“certainly impending.”¹⁶⁰ Specifically, the court reasoned that the employees’ allegations of increased risk of identity theft relied on speculation that the hacker: “(1) read, copied, and understood [the employees’] personal information; (2) intended to commit future criminal acts by misusing the information; and (3) was able to use such information to the detriment of the employees by making unauthorized transactions in the employees’ names.”¹⁶¹ The court further reasoned that in this case, the employees did not show evidence that the intrusion was intentional or malicious.¹⁶² The court focused on the fact that there had been no misuse of the information yet, therefore, no harm had taken place.¹⁶³ The court also highlighted that no identifiable taking occurred because all the court knew was that a firewall had been penetrated.¹⁶⁴

The Fourth Circuit has also rejected the notion that an increased risk of identity theft is sufficient to establish Article III standing.¹⁶⁵ For example, in *Beck*, a laptop containing patients’ unencrypted personal identifying information such as names, birth dates, the last four digits of their Social Security numbers, and physical descriptors was misplaced or stolen.¹⁶⁶ Medical record boxes that contained patients’ names, Social Security numbers, and medical diagnoses also went missing.¹⁶⁷ The patients claimed Article III standing based on an increased risk of future identity theft.¹⁶⁸ The court held that the risk of future identity theft stemming from the incidents was too speculative to satisfy the injury in fact requirement because the plaintiffs failed to allege either (i) that the thief “intentionally targeted” the personal information contained in the laptop and boxes; or (ii) that the thief subsequently used that information to commit identity theft.¹⁶⁹

The court in *Beck* distinguished its case from *Krottner*, *Remijas*, and *Galaria*, cases where the courts had found that increased risk of identity theft was sufficient to establish an injury in fact.¹⁷⁰ The court explained that in *Galaria* and *Remijas*, “the data thief intentionally targeted the personal

---

¹⁶⁰ *Id.* at 43.

¹⁶¹ *Id.* at 42.

¹⁶² *Id.* at 44.

¹⁶³ *Id.* at 42, 44.

¹⁶⁴ *Id.* at 44.

¹⁶⁵ *Beck v. McDonald*, 848 F.3d 262, 277–78 (4th Cir. 2017).

¹⁶⁶ *Id.* at 267.

¹⁶⁷ *Id.* at 268–69.

¹⁶⁸ *Id.* at 273.

¹⁶⁹ *Id.* at 274–75.

¹⁷⁰ *Id.* at 274.

information compromised in the data breaches.”¹⁷¹ In addition, the court highlighted that in *Remijas* and *Krottner*, at least one of the victims of the data breach had already alleged “misuse or access by the thieves” to the personal information stolen in the breach.¹⁷² The court noted that in this case, the patients did not provide any evidence that the information found in the laptop has been accessed or misused, that they suffered identity theft, or that the thief stole the laptop with the intent to steal their private information.¹⁷³

The Fourth Circuit also found the risk of identity theft is not substantial enough to invoke standing unless the victims affected can show the risk was not speculative by showing an attenuated chain of possibilities.¹⁷⁴ For example, in *Beck*, the court also reasoned that for the patients to suffer the harm of identity theft they claimed, the patients had to engage in the same “attenuated chain of possibilities” analysis the Court had rejected in *Clapper*.¹⁷⁵ The court explained that the patients’ alleged identity theft was speculative because the court had to assume that (1) the thieves intended to steal the items to get patients’ personal information, (2) the thieves would then select the named patients’ personal information among all the other patients, and (3) the thieves would successfully use that information to steal the patients’ identity.¹⁷⁶ The court further rejected the patients’ argument that 33 percent of health-related data breaches result in identity theft because those statistics fall short of establishing a “substantial risk” of harm since over 66 percent of the patients will suffer no harm.¹⁷⁷

The Court of Appeals for the Eighth Circuit has also held that an increased risk of identity theft is not sufficient to meet the injury in fact requirement.¹⁷⁸ For example, in *Alleruzzo*, cybercriminals hacked grocery stores’ databases and gained access to the payment card information of customers, including their names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs).¹⁷⁹ The allegedly stolen card information did not include any personally identifying information, such as Social Security

---

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ *Id.* at 275.

¹⁷⁵ *Id.*

¹⁷⁶ *Id.*

¹⁷⁷ *Id.* at 276.

¹⁷⁸ *Alleruzzo v. SuperValu, Inc. (In re SuperValu, Inc., Customer Data Sec. Breach Litig.)*, 870 F.3d 763, 772 (8th Cir. 2017).

¹⁷⁹ *Id.* at 766.

numbers, birth dates, or driver’s license numbers.¹⁸⁰ The customers claimed a heightened chance of experiencing identity theft was their injury in fact.¹⁸¹ The court held that the customers did not show an injury in fact because compromised credit card information could not be used to open unauthorized accounts, which is the type of identity theft generally considered to have a more harmful direct effect on consumers.¹⁸² The court relied on a report released by the United States Government Accountability Office from June 2007 that explained that “credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts.”¹⁸³

In addition, in *Alleruzo*, the court found that the time individuals spend to protect themselves from identity theft after a data breach is not sufficient to establish an injury in fact.¹⁸⁴ In *Alleruzo*, plaintiffs also argued that the costs they incurred to mitigate their risk of identity theft, including the time they spent reviewing information about the breach and monitoring their account information, constitute an injury in fact for purposes of standing.¹⁸⁵ Because the court found that plaintiffs had not alleged a substantial risk of future identity theft, the court also found that the time they spent protecting themselves against this speculative threat cannot create an injury.¹⁸⁶ The court refused to find an injury in fact even though the hackers installed a malware on the company’s network that allowed them to “harvest” the plaintiffs’ credit card information, the company’s practices allowed and made possible the theft of plaintiffs’ card information, and that plaintiffs had actually already suffered theft of their card information.¹⁸⁷

While several federal courts, such as the Second, Third, Fourth, and Eighth Circuit Courts of Appeals, have expressly refused to find an injury in fact based on an increased risk of identity theft in data breach cases, the First Circuit has found that the risk of identity theft is not sufficient to support standing in other situations.

---

¹⁸⁰ *Id.* at 770.

¹⁸¹ *Id.* at 768–69.

¹⁸² *Id.* at 770.

¹⁸³ See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 1, 30 (2007), <http://www.gao.gov/assets/270/262899.pdf> [hereinafter U.S. GOV’T ACCOUNTABILITY OFF.].

¹⁸⁴ *Alleruzo*, 870 F.3d at 771.

¹⁸⁵ *Id.*

¹⁸⁶ *Id.*

¹⁸⁷ *Id.* at 769.

- iv. Although Not in a Data Breach Case, the First Circuit Court of Appeals Has Found that the Risk of Identity Theft Is Not Sufficient for a Plaintiff to Have Standing to Sue in Federal Court.

Although the First Circuit has not addressed whether a plaintiff who was the victim of a data breach suffered an injury in fact based on an increased risk of identity theft, the First Circuit has faced a similar question relating to increased risk of identity theft.¹⁸⁸ For example, in *Katz*, a customer sued a company for allegedly leaving her nonpublic personal information, including social security numbers and taxpayer-identification numbers, unprotected and accessible to prying eyes.¹⁸⁹ Specifically, the customer claimed that the company's users can "access and store her data at home and elsewhere, twenty-four hours a day and seven days a week, in unencrypted form; that the data, once saved by an authorized user, can potentially be accessed by hackers or other third parties; and that the company failed adequately to monitor unauthorized access to her information."¹⁹⁰ Among her alleged injuries, the customer claimed that the company's failure to follow privacy regulations increased her risk of harms associated with the loss of her data, including identity theft.¹⁹¹ The court held that the customer's theory for standing was insufficient because, unlike other cases where courts have found an injury in fact based on a similar theory, the customer's data, in this case, had not actually been accessed by one or more unauthorized parties.¹⁹² The customer's injury was too hypothetical because she only alleged an increased risk that someone might access her data and that if this unauthorized access occurs, then it will increase her risk of identity theft.¹⁹³

Two courts remain that have not yet addressed whether a victim of a data breach has suffered an injury in fact sufficient to have standing to bring a claim in federal court.

---

¹⁸⁸ *Katz v. Pershing, LLC*, 672 F.3d 64, 70 (1st Cir. 2012).

¹⁸⁹ *Id.*

¹⁹⁰ *Id.*

¹⁹¹ *Id.* at 80.

¹⁹² *Id.*

¹⁹³ *Id.*

- v. The Fifth and the Tenth Circuit Courts of Appeals Have Not Analyzed Whether a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.

Almost every Circuit Court of Appeals has addressed whether a plaintiff can establish an injury in fact based solely on the increased risk of identity theft as it relates to data breaches or a printed receipt disclosing a credit card number, in the case of the Eleventh Circuit Court of Appeals. However, the Fifth and Tenth Circuits are the only appeals courts that have not yet addressed the issue.¹⁹⁴

- vi. The Supreme Court Has Refused to Weigh in as to Whether Plaintiffs Who Sue in Federal Court and Claim an Increased Risk of Identity Theft Have Alleged an Injury in Fact.

Despite the federal circuits' divide regarding whether a plaintiff who has been the victim of a data breach has suffered an injury in fact from an increased risk of identity theft, the issue has not been addressed by the Supreme Court even when it has had the chance to do so.¹⁹⁵ The Supreme Court denied certiorari to hear *Attias v. Carefirst*, a case that specifically addressed the issue of whether victims of data breaches have suffered an injury in fact based on an increased risk of identity theft.¹⁹⁶ In *Attias*, customers sued a health insurance company after the company suffered a cyberattack in which its customers' personal information was allegedly stolen.¹⁹⁷ The customers claimed to have suffered an increased risk of identity theft as their injury in fact.¹⁹⁸ The Court of Appeals for the District of Columbia found that the customers alleged a risk of future injury substantial enough to meet the injury in fact requirement of Article III standing.¹⁹⁹ In 2018, the Supreme Court denied certiorari to hear the appeal of this case and failed to answer the circuit split.²⁰⁰

---

¹⁹⁴ Grande, *supra* note 15.

¹⁹⁵ See *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. Aug. 1, 2017), *cert. denied*, No. 17-641, 2018 WL 942459 (U.S. Feb. 20, 2018).

¹⁹⁶ *Id.*

¹⁹⁷ *Id.* at 622.

¹⁹⁸ *Id.*

¹⁹⁹ *Id.* at 626.

²⁰⁰ See *id.*

c. Resolving the Circuit Split

The Supreme Court should resolve the federal district court split and find that a data breach victim has suffered an injury in fact, especially in modern times, where employees can easily work remotely, and an individual's information can get easily exposed to hackers. First, previous Supreme Court decisions regarding injuries in fact support finding that the victim of a data breach has suffered an injury in fact. Second, statistics and legislative action show a correlation between data breaches and identity theft. Third, finding an injury in fact is the equitable result based on the pervasiveness of data breaches and the burden a data breach imposes on a victim. Courts should find that a plaintiff has suffered an injury in fact, even in cases where the stolen information was not found in a database, and instead was found in a laptop or box, and even when the information found is credit card information, such as credit card numbers, PINs, and expiration dates.

- i. The Supreme Court's Previous Decisions that Relate Support a Finding that a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.

The Supreme Court's previous decisions regarding standing support finding that a person who has been the victim of a data breach has suffered an injury in fact. For example, in *Clapper*, the Supreme Court noted that a plaintiff can establish an injury in fact when he or she proves that he or she has a "substantial risk" of suffering the alleged harm.²⁰¹ In *Clapper*, the Court only rejected the plaintiffs' theory of standing because the plaintiffs had to rely on a series of speculative inferences to establish the injury.²⁰² Specifically, the attorneys and human rights, labor, legal, and media organizations had to speculate as to whether intelligence officials would seek to use the surveillance methods under the challenged provision or whether judges would authorize such surveillance.²⁰³ Similarly, in *Lyons*, the Court only rejected a former prisoner's theory of standing because the prisoner challenging a chokehold technique had to assume that he would be arrested and choked by the police again.²⁰⁴ However, these Supreme Court cases support a finding of an injury in fact when a plaintiff has been the victim of

---

²⁰¹ *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013).

²⁰² *Id.* at 410.

²⁰³ *Id.*

²⁰⁴ *City of Los Angeles v. Lyons*, 461 U.S. 95, 105 (1983).

a data breach and personal identifying information, such as names, dates of birth, Social Security numbers, driver’s license numbers, home addresses, telephone numbers, and fingerprint records, has been stolen, because the injury is not speculative.

First, the sole purpose of data breaches is to get access to a victim’s credit card or personal identifying information.²⁰⁵ The next step following a data breach is to use this information in a detrimental way to the customer.²⁰⁶ The most common and well-known way to use that information is by committing identity theft.²⁰⁷ As explained by the Seventh Circuit, the only reason hackers break into a database and steal people’s private information, is to sooner or later assume the customer’s identity.²⁰⁸ Although it might not be completely certain that all of the plaintiff’s stolen data will be used to steal the plaintiff’s identity, a court can find that there is a substantial likelihood that the information will be misused for identity fraud purposes.²⁰⁹ In these types of cases, the data has already been intentionally stolen, therefore the next step for the hackers to benefit from the theft is to use personal information to commit identity theft and fraud.²¹⁰ Once a data breach takes place, the hackers have unlimited access to all the information they need to successfully steal a victim’s identity.²¹¹ The fact that a data breach has already taken place shows the hacker’s intent and ability to use the data in a way that harms the plaintiffs.²¹² In addition, this type of injury is not speculative because the harm, which is to steal the customer’s information with the intent to harm the customer, has already been done. In essence, the substantial risk of harm exists simply by the virtue of the hack and the nature of the personal identifying data stolen.²¹³ The court does not need to engage in the kind of speculative inferences rejected in *Clapper* and *Lyons* to assume that the next natural step following a data breach is to use the data for identity theft and fraud.²¹⁴

In addition, Plaintiffs who claim an increased risk of identity theft because of a data breach face a similar situation to the facts of *Driehaous*,

---

²⁰⁵ Martin, *supra* note 17.

²⁰⁶ *Id.*

²⁰⁷ *Id.*

²⁰⁸ Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

²⁰⁹ Connor Hays, *The Ultimate Guide to Data Breaches*, BLOOM (July 19, 2020), <https://bloom.co/blog/ultimate-guide-to-data-breaches-and-identity-theft/>.

²¹⁰ Remijas, 794 F.3d at 693.

²¹¹ Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017).

²¹² *Id.*

²¹³ *Id.* at 629.

²¹⁴ Clapper v. Amnesty Int’l USA, 568 U.S. 398, 408 (2013); City of Los Angeles v. Lyons, 461 U.S. 95, 105 (1983).

where the Court found the injury was not speculative.²¹⁵ In *Driehaus*, the Supreme Court found that an advocacy group had suffered an injury in fact because the group faced a substantial risk of administrative enforcement of the challenged statute based on the history of past enforcement and because any person with knowledge of the violation of the statute could file a complaint against the advocacy group.²¹⁶ The Supreme Court found standing even when the advocacy group sued based on a political statement that the group had not yet made against a political candidate not yet identified.²¹⁷ The Court found in favor of the advocacy group even when the challenged statute had not yet been enforced against the group nor someone who would file the complaint against the group had been identified.²¹⁸ In that case, the Court did not find the kind of speculative, highly attenuated chain of possibilities it had previously rejected in *Clapper* and *Lyons*, and instead found that the advocacy group had suffered an injury in fact based on the substantial risk of statutory enforcement against them.

Plaintiffs who have suffered a breach of their personal data have an even stronger case for standing to sue than the advocacy group in *Driehaus*.²¹⁹ Similar to the advocacy group in *Driehaus*, the plaintiffs whose personal data has been stolen face a substantial risk of identity theft based on the nature of the personal identifying data stolen, the purpose of data breaches, and the statistics that show a strong correlation between data breaches and identity theft, especially the correlation between data breaches that have compromised personal identifying information and identity theft.²²⁰ The plaintiffs' sensitive information has already been stolen. The next natural step is for the hackers to actually use the information to the victim's disadvantage. It is not speculative or hypothetical to assume that the information will be used for identity theft because that is precisely the purpose of a data breach. Similar to the holding in *Driehaus*, courts do not have to rely on a series of highly attenuated chain of possibilities to conclude that victims of a data breach suffer a "substantial risk" of becoming victims of identity theft.²²¹

---

²¹⁵ Susan B. Anthony List v. Driehaus, 573 U.S. 149, 149–50, 161 (2014).

²¹⁶ *Id.*

²¹⁷ *Id.* at 160–65.

²¹⁸ *Id.* at 161.

²¹⁹ *Id.* at 149–50, 161.

²²⁰ Martin, *supra* note 17; Brandon Bailey, *Pain of Identity Theft on Victim Is Palpable*, DET. FREE PRESS (Dec. 22, 2014, 12:03 AM), <https://www.freep.com/story/money/personal-finance/2014/12/22/identity-theft-victims-personal-information/20612747/> [hereinafter DFP]; Tatham, *supra* note 50.

²²¹ Susan B. Anthony List v. Driehaus, 573 U.S. 149, 149–50, 161 (2014).

Therefore, previous Supreme Court decisions support a finding that plaintiffs who have been the victims of a data breach have suffered an injury in fact based on an increased risk of identity theft.

- ii. The Statistical Correlation Between Data Breaches and Identity Theft and Legislative Action Supports a Finding that a Plaintiff Who Has Been the Victim of a Data Breach Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.

Identity theft is strongly correlated to data breaches. Analysts estimated that in 2014, one in three Americans affected by a data breach ultimately became the victim of financial fraud or identity theft.²²² These statistics show a significant increase in the correlation between data breaches and financial fraud or identity theft from 2010, where it was estimated that one in nine Americans who suffered a data breach then became the victim of identity theft or financial fraud.²²³ In addition, in 2016, 31.7% of data breach victims later became the victims of identity theft, compared to a very low 2.8% of individuals whose information was not involved in a data breach in 2016 and still became the victims of identity theft.²²⁴ In 2018, the number of personal records exposed increased up to 446,515,334 from 197,612,748 in 2017, which analysts correlated to an expected increase in the number of identity theft victims in 2018.²²⁵

Even state legislative actions support the idea that identity theft is highly correlated to data breaches. Specifically, state legislatures have shown that once a person has become the victim of a data breach, the victim has to take certain steps to protect itself from identity theft and fraud.²²⁶ Legislatures have recognized that action needs to be taken after a data breach because of the high correlation between data breaches and identity theft.²²⁷ For example, due to the frequency and severity of data breaches, all fifty state legislatures have passed security breach notification laws.²²⁸ These laws provide citizens

---

²²² DFP, *supra* note 220.

²²³ *Id.*

²²⁴ Tatham, *supra* note 50.

²²⁵ Ana Bera, *50 Shocking Identity Theft Statistics*, SAFEATLAST BLOG (Mar. 6, 2019), <https://safeatlast.co/blog/identity-theft-statistics/#gref>.

²²⁶ *Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (July 17, 2020), <https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

²²⁷ *Id.*

²²⁸ *Id.*

with the right to be notified in a timely manner once their records have been exposed in a data breach.²²⁹ Therefore, statistics and legislative action support a finding that victims of a data breach have suffered an injury in fact based on an increased risk of identity theft.

iii. Courts Should Find that Plaintiffs Who Have Been the Victims of a Data Breach Have Suffered an Injury in Fact Based on an Increased Risk of Identity Theft Because That Is an Equitable Result Based on the Pervasiveness of Data Breaches and the Burden a Data Breach Imposes on a Victim.

Allowing plaintiffs who have been the victims of a data breach to sue in federal court based on an increased risk of identity theft is also an equitable result. Although the purpose of standing is to limit the judiciary power, the purpose of having a judiciary branch is to provide injured parties with redressability and a remedy in court. That is why the Founding Fathers included Article III, Section 1 in our Constitution, creating a judiciary.²³⁰ In this case, it is equitable to allow victims of data breaches to sue in federal court because data breaches become more common every year and victims suffer severe consequences from those data breaches.

1. Pervasiveness of Data Breaches

First, an ever-increasing number of Americans are affected by data breaches yearly. Since 2011, the number of data breaches reported in the United States has been rising.²³¹ For example, in 2013, 614 data breaches were reported.²³² In 2014, that number rose to 783 data breaches.²³³ The number of data breaches in 2016 increased to 1,093, further increasing to 1,579 data breaches reported in 2017.²³⁴ These numbers suggest that data breaches have become more common in recent years, exposing a greater number of individuals to an increased risk of identity theft and to the costs associated with dealing with the consequences of the breach. These numbers also suggest that the number of people who hope for a day in court against the companies that negligently handled their personal data has increased.

---

²²⁹ *Id.*

²³⁰ U.S. CONST. art. III, § 1.

²³¹ De Groot, *supra* note 4.

²³² *Id.*

²³³ *Id.*

²³⁴ *Id.*

The United States is also the country with the highest ratio of data records stolen relative to its population.²³⁵ For example, the United States leads data breach records with 6 billion records stolen and with a ratio of 19 in comparison to its population.²³⁶ South Korea followed the United States with 229 million and with a 4.5 ratio.²³⁷ Next, were Canada and the United Kingdom with 91 and 140 million records stolen compared to 2.5 and 2.1 ratios respectively.²³⁸ Last, was Australia with 50 million records stolen and with a ratio of 2.²³⁹

In addition, data breaches are so pervasive that data stolen in the United States can be used anywhere in the world. For example, in *Whalen*, a customer’s data was stolen in the United States from a purchase she made at Michaels, and her credit card information was presented to make purchases in Ecuador. Because data breaches affect Americans so pervasively and data breaches are strongly correlated to identity theft, victims of data breaches should be found to have suffered an injury in fact to be able to sue in federal court and seek redress for their inconveniences.

2. Mitigation Economic Costs of a Data Breach

Data breaches are also costly and burdensome to the victims.²⁴⁰ As explained by the Sixth Circuit, data breach victims often have to take steps to protect their personal and financial security following a data breach.²⁴¹ In many instances, it may be very difficult and even impossible for the victims to change the information stolen in the breach, such as Social Security numbers, home addresses, or birth dates. In addition, for personal identifying data, victims might have to hire an expert or purchase a software to remove the data from the web, specifically from the “dark web” where cyber hackers are common.²⁴² If the victim does not take these steps, the victim may be at risk of being “victimized repeatedly over time as the data is reused and resold.”²⁴³ Therefore, becoming the victim of a data breach can be unsettling

---

²³⁵ Ron Sobers, *The World in Data Breaches*, VARONIS (Mar. 29, 2020), <https://www.varonis.com/blog/the-world-in-data-breaches/>.

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ *Id.*

²⁴⁰ See *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App’x 384, 388 (6th Cir. 2016).

²⁴¹ *Id.*

²⁴² See Wendy M. Grossman, *The Impact of a Breach: When the Fallout Means More than Money*, INFO SECURITY MAG. (Aug. 21, 2017), <https://www.infosecurity-magazine.com/magazine-features/impact-of-a-breach-more-than-money/>.

²⁴³ *Id.*

and costly. In addition to the costs of data breaches, data breach victims should be allowed to sue in federal courts based on an increased risk of identity theft because data breach victims “may not see the full extent of identity theft or identity fraud” for many years to come.²⁴⁴ Because of the economic costs associated with a data breach to prevent severe consequences such as identity theft, courts should find that a data breach victim has suffered an injury in fact based on an increased risk of identity theft.

3. *Emotional Costs of a Data Breach*

In addition, data breaches have lasting emotional effects on the victims, instilling fear, anxiety, and even danger.²⁴⁵ Following a data breach notice, individuals often experience fear and anxiety that the data breach will lead to identity theft, and anger that the breached entity was so careless with their personal information.²⁴⁶ For example, data breaches of medical records provoke extensive anxiety.²⁴⁷ Victims of medical records data breaches are concerned with issues such as whether medical identity theft will cause them to be refused medical care.²⁴⁸ Because of the lasting emotional effects, a data breach victim can suffer, courts should find that a victim of a data breach has suffered an injury in fact based on an increased risk of identity theft.

iv. Unlike the Fourth Circuit’s Finding in *Beck*, the Victim of a Data Breach from a Stolen Laptop Is Sufficient to Find that the Victim Has Suffered an Injury in Fact Based on an Increased Risk of Identity Theft.

The theory that an increased risk of identity theft resulting from a data breach is sufficient to establish an injury stands even when the item stolen was a laptop with unencrypted personal identifying data. In contrast, in *Beck*, the Fourth Circuit found that patients did not have standing to sue based on an increased risk of identity theft when a laptop and medical record boxes containing the patients’ personal identifying information were stolen.²⁴⁹ The court mainly reasoned that the patients failed to prove that the thief had intentionally targeted the personal information contained in the laptop or

---

²⁴⁴ *In re Zappos.com, Inc.*, 884 F.3d 893, 898–99 (9th Cir. 2018).

²⁴⁵ Grossman, *supra* note 242.

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ *Id.*

²⁴⁹ *Beck v. McDonald*, 848 F.3d 262, 267–69 (4th Cir. 2017).

boxes or that the thief had subsequently used the information to commit identity theft.²⁵⁰ Nonetheless, the only reason why a thief would target boxes that contain personally identifying information is to use that information in some way to their advantage. Empty boxes without the personally identifying information have no value to a thief; therefore, the only plausible reason why those boxes were taken was for the same reason that thieves penetrate encrypted databases. The same reasoning applies to the stolen laptop. The actual device has little value without the personally identifying information that can be used to later steal the patients’ identity and commit fraud. Also, in *Beck*, the fact that the only items stolen were a laptop and a box containing patients’ personally identifying information speaks as to the intent of the thieves. Similar to a breach in an online database, the information necessary to commit identity theft has already been stolen, and the next natural step of the theft is for the thief to use that information in a way that benefits them and harms the victims. Specifically, the next step is for the thief to commit identity theft or fraud.

- v. Unlike the Eighth Circuit’s Decision in *Alleruzzo*, Stolen Credit Card Information Such as Credit Card Number, PIN, and Expiration Date Can Give Rise to an Injury in Fact Based on an Increased Risk of Identity Theft.

An increased risk of identity theft based on credit card data theft is sufficient to find that a data breach victim has suffered an injury in fact. In *Alleruzzo*, cybercriminals hacked grocery stores’ databases and gained access to the payment card information of customers, including their names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs).²⁵¹ The court held that the victims had not suffered an injury in fact based on an increased risk of identity theft because credit card information could not be used to open unauthorized accounts.²⁵² Although credit or debit card information may not be used alone to open new unauthorized accounts, the victims of a data breach of this kind have still suffered an injury in fact.²⁵³ Specifically, plaintiffs’ who have been victims of a data breach giving hackers access to the plaintiffs’ credit card information have suffered an injury in fact because they must spend time and effort monitoring their credit card transactions or canceling

---

²⁵⁰ *Id.* at 274–75.

²⁵¹ *In re SuperValu, Inc.*, 870 F.3d 763, 766 (8th Cir. 2017).

²⁵² *Id.* at 770.

²⁵³ *See* U.S. GOV’T ACCOUNTABILITY OFF., *supra* note 183, at 30.

those credit cards. The information stolen could also be sold on the black market by the hackers. In addition, the plaintiffs have to deal with the mental anguish that their information was stolen and the insecurity that they do not know what the hacker might do with their information. Therefore, even if the information stolen is not personally identifying information, a data breach of credit or debit card information is sufficient to find that a plaintiff has suffered an injury in fact based on an increased risk of identity theft.

IV. CONCLUSION

The Supreme Court should weigh in on the issue and find that a Plaintiff who has been the victim of identity theft has suffered an injury in fact sufficient to grant standing to sue in federal court, agreeing with the Sixth, Seventh, Ninth, and D.C. Circuit Courts of Appeals. First, previous Supreme Court decisions regarding an injury in fact support that finding. Second, statistics and legislative action show a correlation between data breaches and identity theft. Third, finding that a Plaintiff who has been the victim of a data breach has suffered an injury in fact is the equitable result based on the pervasiveness of data breaches and the burden a data breach imposes on a victim, including economic and emotional burden. Courts should also find an injury in fact based on an increased risk of identity theft applies to all victims of a data breach, including data breaches that occurred during a physical laptop or box theft and when the information stolen in the breach is credit or debit card information.

As the use of technology becomes more pervasive, and data breaches and identity thefts become more common, the Supreme Court should settle the issue once and for all and allow victims of a data breach to solve their grievances in federal court. Under our constitution, data breach victims are owed the chance to be heard in court, and the companies that negligently handled their data deserve to be held accountable for their mistakes.