# A PRICE TO PAY: DETERMINING THE OPTIMUM PRICE OF DATA PROTECTION TO ESTABLISH IMMINENT INJURY AND STANDING IN DATA-BREACH CASES

**Katrina B. Do***

## I. Introduction

Attention to the modern-day consumer: it's no longer a question of "if" your personal data will be breached, but "when" your personal data will be breached. In the new digital age consumers are more inclined to place their trust—and their financial and personal information[1]—into the hands of data-storing companies, such as Equifax.[2] This trust likely stems from a reasonable expectation that companies will take preventative measures to ensure the safety of their customers' private and sensitive information.[3] Unfortunately, this expectation has become increasingly unreasonable with the uptick of data-breaches.

The recent Equifax breach, named one of the gravest data security breaches in history, revealed how flimsy customers' beliefs of data security and privacy can be.[4]

---

* J.D. Candidate (May 2019), The John Marshall Law School. I would like to thank my grandmother (my "a Ba") for pouring down love and guidance at every step of my law school career, and my parents for always encouraging me to explore the world beyond the comforts of home.

[1] *See* Arthur R. Vorbrodt, Article, *Clapper Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison*, 73 WASH. & LEE L. REV. ONLINE 61, 63 (discussing the growing sophistication of online hackers and noting the dozens of recent commercial data breaches); IDENTITY THEFT RES. CTR., DATA BREACH REPORTS: 2016 END OF YEAR REPORT 4 (2017) [hereinafter 2016 Data Breach Reports], https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf; IDENTITY THEFT RES. CTR., DATA BREACH REPORTS 4 (2015), www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

[2] Equifax is one of the nation's three major credit-reporting agencies, which store and analyze consumers' financial history for credit decisions. CONSUMER FINANCIAL PROTECTION BUREAU, LIST OF CONSUMER REPORTING COMPANIES (2018).

[3] Cristiana Modesti, Note, *Incentivizing Cybersecurity Compliance in the New Digital Age: Prevalence of Security Breaches Should Prompt Action by Congress and the Supreme Court*, 36 CARDOZO ARTS & ENT. L.J. 213, 214 (2018).

[4] Bob Sullivan, *Your Social Security Number Isn't a Secret*, N.Y. TIMES (Sept. 13, 2017), www.nytimes.com/2017/09/13/opinion/your-social-security-number-isnt-a-secret.html (arguing Social Security

The hacking of Equifax's data compromised sensitive information, including Social Security Numbers of at least 143 million consumers.[5] Equifax, primarily in the business of storing consumer data, failed at its one job.[6] A data-storage credit agency lost 143 million consumers' data; yet the company is performing business as usual, and hundreds of millions of Americans affected by the breach are left with shaky options for legal recourse.[7]

This is the data-breach problem: an alarming number of data-breaches and an equally alarming lack of adequate and consistent legal response. In the typical data-breach scenario, consumers fight back by filing class action lawsuits against private companies that have experienced data-breaches. However, the data-breach plaintiff is generally unsuccessful, in part because courts lack a unified approach to finding injury-in-fact sufficient to create standing in data-breach instances.

The Supreme Court has yet to provide a clear standard for determining standing in data-breach cases.[8] As a result, confusion reigns supreme among the lower courts in this area. The growing circuit court split involves whether a data-breach plaintiff's alleged risk of future harm, or some other factor, is an injury-in-fact

---

numbers were never designed to be a security tool, and their purpose for such has run its course following the Equifax breach).

[5] Aodhan Beirne, *'A Problem With No End in Sight': Readers' Exasperation With Equifax*, N.Y. TIMES (Sept. 14, 2017), www.nytimes.com/2017/09/14/reader-center/equifax-questions.html.

[6] Farhad Manjoo, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. TIMES (Sept. 8, 2017), www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html.

[7] *Id.*

[8] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (rejecting, indirectly, standing based on an increased risk of future identity theft in its decision, its application is unclear, given its factual context).

sufficient to establish standing.[9] On one side of the split, circuit courts found standing based on an increased risk of future identity theft; circuit courts on the other side of the issue found such an injury too speculative to constitute standing.[10] As the Equifax litigation begins, and hacked data continues to surface, these split decisions will affect how victims of data-breaches may bring claims against a company.

As long as the digital world continues to exist, data-breaches will continue. Although legislatures play a role in regulating procedures that may help reduce the risk of data-breaches,[11] preventative measures are not enough. This Comment addresses the need for relief when the inevitable data-breach occurs and proposes a framework in which the judiciary may determine injury-in-fact from an economic perspective. Part I of this Comment introduces the basic principles of Article III standing under the United States Constitution. Part II discusses the circuit split regarding whether injury exists in data-breach cases. Part III examines the expenses that one incurs when their information is exposed in a data-breach. While certain

---

[9] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690-91 (7th Cir. 2015) (holding customers satisfied Article III standing requirements based on some injuries they identified where allegations of future harm due to a security breach by the store survived a motion to dismiss); Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 959 (S.D. Cal. 2014); In re SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017) (holding that plaintiffs' complaint did not sufficiently allege a substantial risk of identity theft, and plaintiff customers' allegations of future harm were not sufficient to support standing).

[10] *Compare* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 385 (6th Cir. 2016) (finding standing based on increased risk of identity theft), *and* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016), *with* Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (finding increased risk of identity theft insufficient for standing), *and* Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).

[11] *See* Tara Siegel Bernard, *After Equifax Breach, Credit Freeze Provision Comes at a Price*, N.Y. TIMES (Mar. 15, 2018), www.nytimes.com/2018/03/15/your-money/equifax-breach-credit-freezes.html (discussing a provision in a Senate financial regulation bill that would make credit freezes free for consumers, with the caveat that the bill would also override state laws that could potentially provide more consumer protection).

future expenses have been argued to be speculative calculations from a monetary standpoint, this Comment will argue that a price can be put on data protection, and that some data may be cheaper to lose than others.[12] Finally, this Comment will conclude with a list of factors courts should consider in determining the injury sufficient to establish standing.

## II. Background

This section begins with a background on the nature of data-breach class action suits and the three prongs of Article III standing. It continues with an overview of the circuit court split regarding injury-in-fact for data-breach plaintiffs, and how the Supreme Court decision in *Clapper v. Amnesty International* further muddied the water for data-breach litigation.[13]

### A. Data-Breaches: The Latest Trend in Class Actions

Data privacy and security are suspected as the area of law most likely to give rise to the next wave of class action litigation.[14] Typically, data-breach actions are brought as class actions because of the sheer number of individuals affected and the small amount of damages involved.[15] Most data-breach actions are brought in federal

---

[12] For example, a person who loses an email password could potentially lose the password to their bank account if that person uses the same password for multiple accounts.

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

[14] Megan Dowty, Note, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683 (citing THE 2015 CARLTON FIELDS JORDEN BURT CLASS ACTION SURVEY 9 (2015), https://classactionsurvey.com/pdf/2015-class-action-survey.pdf.). *But see* THE 2017 CARLTON FIELDS JORDEN BURT CLASS ACTION SURVEY 2 (2017), www.classactionsurvey.com/pdf/2017-class-action-survey.pdf (noting that data privacy actions, while highly anticipated in the last several years, remained a small percentage of overall class actions).

[15] Dowty, *supra* note 13; *see also* Stacy Cowley, *2.5 Million More People Potentially Exposed in Equifax Breach*, N.Y. TIMES, Oct. 2, 2017, https://www.nytimes.com/2017/10/02/business/equifax-breach.html (reporting additional

court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) (2012), which extends federal diversity jurisdiction to all class actions where minimal diversity exists and the amount in controversy exceeds $5 million.[16]

1. Low Success Rate

Data-breach class actions have generally been unsuccessful. Courts tend to dismiss a large number of these lawsuits because plaintiffs cannot establish a cognizable injury-in-fact, which is required for Article III standing.[17] This is especially true in cases where plaintiffs allege increased risk of future harm from their compromised data.[18] For example, in *In re United States OPM Data Sec. Breach Litigation*,[19] data-breach cases arising from a cyberattack on millions of federal employees were dismissed for lack of jurisdiction because plaintiffs failed to show an economic harm resulting from the breach; incurring certain costs as a reasonable reaction to the breach did not constitute a cognizable injury-in-fact.[20] When purported

---

compromised accounts were found during a forensic investigation by a cyber security firm, adding 2.5 million data breach victims to the existing 145.5 million originally estimated).

[16] The Class Action Fairness Act of 2005 (CAFA) grants district courts original jurisdiction over any civil action involving a proposed class of at least 100 members in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which any member of a class of plaintiffs is a citizen of a State different from any defendant. 28 U.S.C. § 1332(d).

[17] *See*, *e.g.*, Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (finding no Article III standing because plaintiffs in consolidated suits could not show an impending threatened harm of future identity theft and no showing of substantial risk that a harm would occur and require mitigation costs); U.S. CONST. art. III.

[18] *See* Beck, 848 F.3d 262; *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3rd Cir. 2011) (denying standing in a data breach case where plaintiffs could not satisfy the injury-in-fact requirement, stating that "allegations of an increased risk of identity theft as a result of the security breach [were] hypothetical, future injuries, and [were] therefore insufficient to establish standing.").

[19] In re United States OPM Data Sec. Breach Litig., 266 F. Supp. 3d 1 (D.D.C. 2017).

[20] *Id.* at 36.

data-breach class actions are filed in federal court, the first obstacle is likely whether the plaintiff class has standing to sue under Article III of the U.S. Constitution.[21]

B. Article III Standing

The Constitution establishes Article III standing as a "threshold question in every federal court case."[22] While the Constitution does not explicitly mandate "standing" to file a federal lawsuit, the Supreme Court has interpreted Article III's language of limiting judicial decisions to "cases" and "controversies" to mean that federal courts must require standing to show that plaintiffs have a genuine interest and stake in the outcome of litigation.[23] Federal court jurisdiction requires standing for each claim of relief sought.[24]

To bring a "case or controversy" in federal court, a plaintiff must establish three elements of standing. First, a plaintiff must have suffered an injury-in-fact,

---

[21] *See* U.S. CONST. art. III, § 2.

[22] U.S. CONST. art. III; United States v. Bearden, 328 F.3d 1011, 1013 (8th Cir. 2003).

[23] The Constitutional standing requirements, derived from Article III, Section 2, provides:

> "The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority; - to all Cases affecting Ambassadors, other public Ministers and Consuls; - to all Cases of admiralty and maritime Jurisdiction; - to Controversies to which the United States shall be a Party; - to Controversies between two or more States; - [between a State and Citizens of another State; - ] between Citizens of different States, - between Citizens of the same State claiming Lands under Grants of different States, [and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.]".

U.S. CONST. art. III, § 2; *see also* Stark v. Wickard, 321 U.S. 288, 310 (1944) (stating Article III grants courts the power to "adjudicate cases and controversies as to claims of infringement of individual rights whether by unlawful action of private persons or by the exertion of unauthorized administrative power").

[24] *See* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 352 (2006) (stating "a plaintiff must demonstrate standing separately for each form of relief sought." (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 185 (2000) (internal quotation marks omitted))).

which must be "actual" and "imminent." This is the most difficult prong to establish in data-breach actions. Second, the plaintiff's injury must be fairly traceable to the defendant's action. Third, a decision in the plaintiff's favor must be able to redress the alleged harm. The plaintiff has the burden of proof of establishing these elements.[25]

1. Three-Prong Test

The Supreme Court has established a three-prong inquiry as to whether Article III standing exists in a federal case. To bring a "case or controversy" in court, a plaintiff must suffer an injury that is: (1) "concrete, particularized, and actual or imminent"; (2) "fairly traceable to the challenged action"; and (3) "redressable by a favorable ruling."[26] The first element is the biggest roadblock for plaintiffs in data-breach actions. This element requires the plaintiff to suffer an "injury in fact" that is "concrete and particularized" and not "conjectural" or "hypothetical."[27]

a. First Prong is the Worst Prong: The Injury Roadblock

Historically, the injury-in-fact prong of the Article III standing test has presented the biggest roadblock for plaintiffs in data-breach cases.[28] The most common theory of harm on which plaintiffs rely is the allegation of an increased risk

---

[25] Patricia Cave, Comment, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 772 (2013) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)).
[26] Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010).
[27] Whitmore v. Arkansas, 495 U.S. 149, 155 (1990).
[28] *See* Lexi Rubow, Note, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 BERKELEY TECH. L.J. 1007, 1040-42 (2014) (advocating for broader standing requirements in data breach cases).

of future identity theft or fraudulent charges by nature of their personal information being stolen. A plaintiff usually alleges that the defendant-company's failure to protect plaintiff's personal information has increased the plaintiff's risk of future harm of identity theft, and therefore, the plaintiff has increased costs of taking precautionary measures to prevent the future harm from occurring.[29] A number of the early circuit court decisions to face this issue refused to find increased risk of future identity theft to support standing.[30] However, not all the courts followed this early trend. In 2007, the Seventh Circuit found standing in *Pisciotta v. Old National Bancorp*.[31]

The injury-in-fact prong relates to a plaintiff's claim of monetary damages resulting from the data-breach. Specifically, the injury-in-fact requirement is at issue when the plaintiff's information was stolen but was not used to make purchases. For example, in 2013, hackers obtained credit card and other personal information of 110 million Target customers. [32] The hackers used this stolen credit card information to make fraudulent purchases thereafter. The plaintiff-customers alleged "that they actually incurred unauthorized charges; lost access to their accounts; and/or were forced to pay sums such as late fees, card-replacement fees, and credit monitoring

---

[29] Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 414-19 (2014) (examining the problems posed by data breach lawsuits).

[30] *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) ("In this increasingly digitized world, a number of courts have had occasion to decide whether the 'risk of future harm' posed by data security breaches confers standing on a person whose information may have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative.").

[31] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

[32] *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

costs because the hackers misused their personal financial information."[33] These concrete monetary expenses should constitute an injury, as the Eighth Circuit district court held in *In re Target*.[34]

2. Types of Injuries

a. Direct Harm

Data-breach cases may involve different types of alleged injuries. In the first type of injury allegation, the plaintiff alleges a third-party stole information, and that third-party has used the plaintiff's information to make additional charges and purchases.[35] In *Lambert v. Hartman*, the Sixth Circuit found that the plaintiff established injury-in-fact when she incurred fraudulent charges from a third-party who obtained her information through a data hack.[36] The *Lambert* case involved a ticket for a traffic violation that was posted on a website accessible to the public.[37] The traffic ticket included sensitive and personal information about the plaintiff, which the hacker was able to easily access and use to make purchases on the plaintiff's credit card.[38]

Injury-in-fact is generally established in cases where fraudulent purchases have directly harmed the plaintiff.[39] These types of actions—where the plaintiff can

---

[33] *Id.* at 1158.
[34] *Id.* at 1158-59.
[35] Caroline C. Cease, Note, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 414-19 (2014) (addressing the standing concern in data breach actions).
[36] Lambert v. Hartman, 517 F.3d 433, 433, 435-36 (6th Cir. 2008).
[37] *Id.* at 435-36.
[38] *Id.*
[39] *See id.* at 437 (finding that plaintiff met injury-in-fact requirement when actual charges were made on her account).

establish injury-in-fact by a show of the plaintiff's "actual financial injuries"[40]—do not pose issues to establishing standing in data-breach cases.

b. Indirect Harm

The second type of injury is when the plaintiff's information has been accessed but not used to make unauthorized purchases or open unauthorized accounts.[41] The main distinction between this type of injury and the first is that a plaintiff has difficulty showing economic harm in the second type of injury—where no third-party has caused any direct harm to the plaintiff's bank account or personal information. This indirect harm may include an allegedly increased risk of identity fraud and the costs associated with obtaining security protection, such as credit-monitoring procedures.

These credit-monitoring procedures include not only purchasing credit-monitoring services, but also less calculable expenses, including but not limited to: personal time expended canceling credit cards and opening new ones; changing passwords and usernames or email addresses; calling companies directly to verify information; closing banking accounts and starting new accounts (if the bank account number was exposed); reporting to banks; having a credit-reporting agency place a fraudulent alert on the plaintiff's account (if the plaintiff's social security number was exposed); placing credit freezes on one's account; inserting new card information into

[40] *Id.* (reasoning that plaintiff's allegation that her identity was stolen, and her credit rating and financial security suffered as a result was sufficient to establish injury-in-fact).
[41] Cease, *supra* note 35, at 399.

plaintiff's auto-fill program; and changing recurring payment methods.[42] In addition to these harms, plaintiffs have also alleged suffering a loss of rewards points on credit cards and enduring general anxiety that their information may be compromised in the future to make unauthorized purchases.[43] The issue in these cases centers around whether an increased risk of identity fraud and credit-monitoring procedures are sufficient to constitute an injury.[44]

C. Circuit Court Split

1. Heart of the Circuit Court Confusion: The Supreme Court Decision in *Clapper v. Amnesty International USA*

In 2013, the United States Supreme Court, in *Clapper v. Amnesty International USA*,[45] held that a plaintiff who alleges future injuries resulting from a defendant's improper conduct must prove that such injuries are "currently impending."[46] *Clapper* involved allegations that a section of the Foreign Intelligence Surveillance Act (FISA)[47] was unconstitutional.[48] The plaintiffs—including media organizations and human rights groups—argued injury-in-fact because of the increased likelihood that FISA would intercept their communications in the future.[49]

---

[42] *See What Should I Do if I Have Been a Victim of a Data Breach?*, TIME: MONEY (May 26, 2014), www.time.com/money/2791976/data-breach-victim.
[43] *See* 3 IAN C. BALLON, E-COMMERCE AND INTERNET LAW § 27.07 (2d ed. 2009).
[44] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (holding that the plaintiffs' allegations of incurred expenses for credit-monitoring services as a result of hacked personal information passed the standing inquiry, despite the lack of allegations that hackers actually used this information).
[45] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[46] *Id.* at 401.
[47] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §1881(a) (2012).
[48] *See Clapper*, 568 U.S. at 420.
[49] *Id.* at 410.

The plaintiffs also claimed they spent significant costs to protect the confidentiality of their communications and to avoid having those communications intercepted by FISA, claiming these measures taken constitute a present injury to establish standing.[50]

Regarding the first argument, that plaintiffs will suffer future harm, the Court found no injury-in-fact because that standing theory would "require guesswork" that the Court was not willing to endorse.[51] The Court also noted the importance of the requirement that an injury is "certainly impending," citing *Whitmore v. Arkansas*.[52] The Court rejected the plaintiff's second argument that plaintiffs suffered immediate harm by taking precautionary measures to avoid potential communication interception.[53] The Court reasoned that this allegation did not meet the injury-in-fact requirement because the plaintiffs could not "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending," and that "the costs they have incurred to avoid surveillance are simply the product of their fear of surveillance."[54] The Court stated that the plaintiffs failed to provide concrete evidence that their fears of government surveillance were legitimate, but instead relied more on "conjecture about possible governmental actions."[55]

---

[50] *Id.*
[51] *Id.* at 413.
[52] *Id.* at 409; Whitmore v. Arkansas, 495 U.S. 149, 157-60 (1990).
[53] *Clapper*, 568 U.S. at 413.
[54] *Id.* at 416-17.
[55] *Id.* at 420.

Since *Clapper*, lower courts have been split in data-breach cases on whether plaintiffs have standing to sue the party who failed to protect their data.[56] Although *Clapper* involved foreign surveillance, the question of standing in data-breach cases still relates here because the Court's standing analysis provides insight on the injury-in-fact requirement in data-breach litigation.[57] Similar to *Clapper*, plaintiffs in data-breach cases often allege fear of future harm about how a third- party may act.[58] An increased fear that leads a plaintiff to take precautionary measures to protect their identity and sensitive financial information is similar to the *Clapper* plaintiffs who failed to show injury-in-fact by "inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[59]

2. The Lower Courts Before and After *Clapper*

*Clapper* did not explicitly address injury-in-fact as it relates to data-breach actions, but some lower courts have interpreted it as a standing doctrine that limits

[56] Bradford C. Mank, *Data Breaches, Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits?*, 92 NOTRE DAME L. REV. 1323, 1327 (2017) (discussing the split circuits following the Supreme Court decision in Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013), noting that a majority of the lower federal courts in data breach cases where there is no proof of misuse or fraud have held that plaintiffs lack standing to sue the party who failed to protect their data, while on the other hand, a significant minority of lower federal courts have held that plaintiffs do have standing in these instances).

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

[58] *Id.* at 415; *see also* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (holding plaintiffs' allegations of incurring expenses from purchasing credit monitoring services as a result of a data breach passed the standing inquiry) ("[T]he injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiffs only by increasing the risk of future harm that plaintiffs would have otherwise faced, absent the defendant's actions.").

[59] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013).

plaintiffs from alleging claims of future injury.[60] However, one thing is clear: *Clapper* only added insult to injury with its decision by widening the already-split circuits on how to rule on standing in data-breach cases.[61]

a. Courts Allowing Standing Before *Clapper*

Several cases allowed standing before *Clapper*.[62] In *Pisciotta v. Old National Bancorp*, the Seventh Circuit held that the plaintiff's allegations of future harm were sufficient to confer Article III standing.[63] *Pisciotta* was a data-breach case involving a defendant bank.[64] The Seventh Circuit acknowledged, in its brief discussion about standing, that several other circuit courts have found that Article III standing is satisfied with a show of future threat of harm.[65] The Seventh Circuit disagreed with district courts that denied Article III standing in data-breach cases because a breach without actual harm was an insufficient injury-in-fact to constitute standing.[66] The *Pisciotta* court stated: "As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future

---

[60] *See Clapper*, 568 U.S. at 415. *See* Thomas Martecchini, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After Clapper v. Amnesty International USA*, 114 MICH. L. REV. 1471, 1483 (2016) (discussing district courts' conflicting interpretations of *Clapper*).
[61] *See id.* The Circuit Court split regarding standing in data breach cases was prevalent before *Clapper* was decided. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (allowing standing in a data breach case involving a plaintiff's threat of future harm); *see also* Beaudry v. TeleCheck Servs., Inc., 579 F.3d 702 (6th Cir. 2009).
[62] *Clapper*, 568 U.S. at 398. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (permitting standing.based on increased risk of harm before *Clapper*).
[63] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639-40 (7th Cir. 2007).
[64] *Id.* at 631-32.
[65] *Id.* at 634.
[66] *Id.* (acknowledging four federal district court decisions from different jurisdictions that denied standing in data breach cases because no actual harm was shown).

harm that the plaintiff would have otherwise faced, absent the defendant's actions."[67] The Seventh Circuit further cited circuit opinions that followed this reasoning in the case footnotes.[68]

Similarly, in *Krottner v. Starbucks Corp.*, the Ninth Circuit held that the plaintiffs' anxiety and stress resulting from a data-breach, along with a threat of future harm of identity theft, was sufficient to meet injury-in-fact under Article III standing requirements.[69] In *Krottner*, a third party stole a laptop from Starbucks Corporation ("Starbucks"), the defendant.[70] The laptop contained sensitive information, including social security numbers, names, and addresses, of approximately 97,000 Starbucks employees.[71] The plaintiffs, Starbucks employees, alleged that the stolen laptop increased their risk of harm of identity theft in the future.[72] Although the plaintiffs did not provide concrete evidence that their stolen information was misused, one plaintiff alleged general feelings of "anxiety and stress" from the incident, and two other plaintiffs alleged injury due to future credit-monitoring expenses.[73] The *Krottner* court held that general anxiety and

---

[67] *Id.*
[68] *Id.* at 634 n.3-4. *Pisciotta* cited decisions from the Second, Fourth, Sixth, and Ninth Circuits that recognized standing for future harm from exposure to toxic substances and medical implants, n.3. The court cited other Seventh Circuit opinions that held a future risk of harm was sufficient to establish standing, provided that the probability of the future injury is more than conjectural, n.4. Based on footnotes three and four, the Seventh Circuit implied that future harm was a sufficient injury in data breach cases if the plaintiff could establish a slight probability that the future harm was likely to occur; *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (noting that after the *Clapper* decision, district courts were split as to whether to apply *Pisciotta* to standing in data breach cases).
[69] Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010) (holding plaintiffs' allegation of future harm of identity theft was sufficient to establish injury-in-fact under Article III).
[70] *Id.* at 1140.
[71] *Id.*
[72] *Id.* at 1142.
[73] *Id.* at 1141.

stress from the laptop theft constituted a present injury that met Article III standing requirements.[74] The court also held that future credit-monitoring expenses and increased risk of future harm were enough to establish the injury-in fact-requirement.[75]

b. Third Circuit Rejecting Standing Before *Clapper*

The Third Circuit, on the other hand, rejected the argument that increased risk of future harm was sufficient to confer Article III standing.[76] In *Reilly v. Ceridian Corp.*, two law firm employees brought a punitive class action lawsuit against Ceridian Corporation, the defendant payroll processing company, after an unknown third party hacker retrieved sensitive information of 27,000 employees at 1,900 different companies, including plaintiffs'.[77] The *Reilly* plaintiffs alleged multiple claims, including that they had an increased risk of identity theft, incurred costs from purchasing credit-monitoring services, and suffered emotional

[74] *Krottner*, 628 F.3d at 1142 (citing Doe v. Chao, 540 U.S. 614 (2004)).
[75] Krottner v. Starbucks Corp., 628 F.3d 1139, 1142-43 (9th Cir. 2010) ("If a plaintiff faces 'a credible threat of harm,' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III." (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002); and L.A. v. Lyons, 461 U.S. 95, 102 (1983))). The court also recognized that in *Pisciotta* the plaintiffs' only alleged harm was the threat of future injury from the increased risk that their information may be misused in the future, plaintiffs did not show any actual financial harm. *Krottner*, 628 F.3d at 1142 (discussing Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007)).
[76] Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (holding "plaintiffs' allegations of hypothetical, future injury were insufficient to" meet Article III standing requirements, and unless and until these hypothetical injuries came true, the plaintiffs suffered no injury-in-fact).
[77] *Id.* at 40. The hacker in this case retrieved plaintiffs' personal and financial data from Ceridian's computer system. It is unknown whether the hacker used any of this data.

distress.[78] The Third Circuit affirmed the decision of the district court,[79] holding that plaintiffs failed to establish Article III standing because of plaintiffs' "allegations of hypothetical, future injury."[80] In its analysis, the *Reilly* court criticized both the *Pisciotta* and *Krottner* decisions for applying the incorrect standing test and did not require an "imminent" or "certainly impending" requirement.[81] The Third Circuit reiterated that instead of requiring an injury to be "certainly impending," the two courts "simply analogized data-security-breach situations to defective-medical-device, toxic-substance-exposure, or environmental-injury cases."[82]

## III. Analysis

### A. Overview: Determining the Price of Data from an Economic Theory

Determining the price of data protection, including the cost of losing specific personally identifying information, is key to understanding whether an injury-in-fact exists. Some courts have held that future costs resulting from data-breaches are

---

[78] *Id.* The plaintiffs filed suit on behalf of themselves, and others similarly situated.
[79] *Id.* The district court dismissed the plaintiffs' claims for lack of Article III standing, as well as for a failure to state a claim on the merits because plaintiffs could not adequately establish the injury and damage elements of each of their claims, *id.* at 41.
[80] *Id.* at 41-46 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)) (using the 1990 Supreme Court decision in *Whitmore* to support the idea that threatened injuries must be "certainly impending" for future allegations of injury to suffice under Article III standing. The injuries must also be imminent to avoid suits based on hypothetical or speculative scenarios.). *Reilly*, 664 F.3d at 42.
[81] *Reilly*, 664 F.3d at 44-46; Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010) (holding plaintiffs' allegation of future harm of identity theft was sufficient to establish injury-in-fact under Article III).
[82] Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011). The court argued that analogizing data breach scenarios to defective medical devices or toxic substances was incorrect because the former cases involve serious harm to human health, *id.* at 44-46.

sufficient to establish an imminent injury required by Article III;[83] other courts refuse to confer standing for alleged future harms. [84] The latter courts are unwilling to consider the costs that plaintiffs incur from canceling bank accounts, applying for new credit cards, and freezing existing accounts (among other things) as sufficient injuries. These already-incurred harms are the product of a data-breach, and they should not be characterized as a self-imposed expense. Taking adequate steps to ensure the integrity of the plaintiffs' financial and personal information is critical following a data-breach; plaintiffs should be able to recover from these losses. As the court in *Remijas v. Neiman Marcus* pointed out, it should be presumed that a hacker's intent, when stealing personal and financial information, is to use that information fraudulently in the future.

This analysis begins by diving deeper into the effects of *Clapper* and how lower courts have interpreted its holding in data-breach cases.[85] Next, it introduces the economic theory and how it compares to the legal theory. This Comment is primarily based on conferring standing by looking at the plaintiffs' injuries from an economic standpoint. The analysis attempts to put a price on the "privacy cost" of data-breach plaintiffs—that is, the plaintiffs' expected costs from tangible and intangible expenses—and how courts can incorporate the privacy cost from an

---

[83] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690-91 (7th Cir. 2015) (holding plaintiff customers satisfied Article III standing requirements when plaintiffs' personal data was stolen from the defendant retailer based on fraudulent charges against some of the plaintiffs, the reasonable potential for future fraudulent charges against all plaintiffs, and the plaintiffs' expenses for credit monitoring services).

[84] *But see Remijas*, 794 F.3d at 694 (mentioning that credit-monitoring services come at a price that easily qualifies at a concrete injury and offering the example that Experian offers credit-monitoring services for $4.95 for the first month, and $19.95 monthly thereafter).

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

economic standpoint to determine whether a sufficient injury exists for Article III standing purposes. The goal of this analysis is to examine a data-breach plaintiff's potential harms from an economic viewpoint and to determine how that analysis fits in the grand scheme of establishing standing in data-breach litigation.

B. *Clapper's* "Certainly Impending" Standard and Appellate Court Decisions

*Remijas v. Neiman Marcus* is a prominent case in which a circuit court distinguished *Clapper* and allowed standing for allegations of future injury.[86] The Seventh Circuit held that the future risk of identity theft and credit card fraud was real and imminent. The court conferred standing by way of an assumption that the hackers' intent in stealing the plaintiffs' information was to use that information fraudulently in the future.[87] Although the plaintiffs had not yet received fraudulent credit card charges or faced identity theft, they alleged:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[88]

*Remijas* distinguished *Clapper*, where plaintiffs lacked evidence that their communications were being monitored. The plaintiffs in *Remijas* were notified of

[86] *Id.*
[87] *Remijas*, 794 F.3d at 693-94.
[88] *Id.* at 692.

the breach and were offered one year of credit-monitoring services, which was a reflection of the seriousness of the breach.[89]

By contrast, a number of district courts have refused to confer standing for allegations of future injury using *Clapper's* "certainly impending" standard. These cases are further analyzed in the sections below.

Although the Supreme Court has not directly addressed the issue of establishing a cognizable injury-in-fact per Article III standing in data-breach cases, lower federal courts have looked to the Court's decision in *Clapper* to interpret whether standing exists in such cases.[90] Some lower courts have interpreted the *Clapper* decision's "certainly impending"[91] standard in data-breach cases to require proof of actual injury and to dismiss cases where only allegations of future injury exist.[92] However, the trend of the appellate court decisions following *Clapper* is a finding of sufficient injury-in-fact to establish Article III standing. First, this Comment looks to a lower court decision that applied the strict standard seen in

---

[89] Cristiana Modesti, Note, *Incentivizing Cybersecurity Compliance in the New Digital Age: Prevalence of Security Breaches Should Prompt Action by Congress and the Supreme Court*, 36 CARDOZO ARTS & ENT. L.J. 213, 223-24 (2018).

[90] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 440 (2013) (Breyer, J., dissenting).

[91] *Id.* at 409 (majority opinion) ("To establish U.S. Const. art. III standing, an injury must be: concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling. Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for U.S. Const. art. III purposes–that the injury is certainly impending. Thus, threatened injury must be certainly impending to constitute injury-in-fact, and allegations of possible future injury are not sufficient.").

[92] John L. Jacobus & Benjamin B. Watson, *Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 3 at 50-61 (2014).

*Clapper*. Next, the Comment moves on to evaluate the cases more in line with the economic-based proposal, in which courts allowed standing for future harms.

1. After-*Clapper*: Refusing to Confer Standing

a. *Green v. eBay Inc.*: A District Court Decision

*Green v. eBay Inc.* clearly stands for the proposition that an increased risk of future harm is not sufficient to create Article III standing.[93] The case comes from the Eastern District of Louisiana, but the opinion is unique because it provides a list of factors to consider in determining whether an injury-in-fact exists for data-breach actions. The factors that the court used in determining whether plaintiffs suffered an injury-in-fact included "whether [the plaintiffs'] data was actually taken when it was accessed, whether certain information was decrypted, whether the data was actually misused or transferred to another third party and misused, and whether or not the third party succeeded in misusing the information."[94]

The court found the plaintiff did not have a substantial stake in the litigation to confer concrete and particularized harm for Article III standing. Moreover, the court rejected the argument that the hackers' only purpose was to use the plaintiffs' information fraudulently in the future, holding that this notion is irrelevant if the threat of future harm is not "certainly impending."[95] This case clearly follows the strict standard in *Clapper*, denying standing where plaintiffs allege an increased risk of future harm.

---

[93] Green v. eBay Inc., No. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2015).
[94] *Id.* at *19.
[95] *Id.* at *5.

2. After-*Clapper*: Finding Sufficient Injury

a. Sixth Circuit Court of Appeals in *Galaria v. Nationwide Mutual*

In 2016, the Sixth Circuit Court of Appeals in *Galaria v. Nationwide Mutual* found that plaintiffs alleged a sufficient risk of harm when their data was stolen and was already "in the hands of ill-intentioned criminals."[96] Given this fact, the Sixth Circuit reasoned that there was no need to speculate whether a future injury would occur.[97] The data-breach contained personal information; in such circumstances, a reasonable inference can be drawn that the hackers will use the victims' personal information for fraudulent purposes.[98] The court continued to reason that Nationwide, the defendant insurance company, knew the seriousness of the risk of injury when the insurance company offered to provide credit-monitoring and identity protection services to those affected by the breach.[99]

While acknowledging the possibility that the criminal hackers would not misuse the plaintiffs' personal information, the court determined that requiring plaintiffs to essentially wait for a misuse of their information would be unreasonable.[100] In summary, the Sixth Circuit held when plaintiffs lost control of their personal data, they did not have to wait to receive some notification of a

---

[96] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) (holding that plaintiffs' allegations of substantial harm and reasonably incurred mitigation costs are sufficient to establish injury for Article III standing purposes).
[97] *Id.*
[98] *Id.*
[99] *Id.* (stating that Nationwide offered credit-monitoring services and identity-protection services for a full year).
[100] *Id.* (reasoning that while actual misuse of plaintiffs' data is not "literally certain," there is still a substantial risk of harm).

fraudulent credit charge before taking steps to mitigate against the future harm, especially when Nationwide recommended taking these steps to ensure their financial and personal security.[101] The court considered plaintiffs' allegations of loss of time and money—through credit monitoring, changing bank and financial accounts, and credit-freezing—to constitute a concrete injury to establish standing.[102]

b. Seventh Circuit Court in Remijas v. Neiman Marcus

The Sixth Circuit in *Galaria v. Nationwide Mutual* noted that its conclusion was "in line" with the Seventh Circuit's decision in *Remijas v. Neiman Marcus Grp., LLC*.[103] In *Remijas*, the Seventh Circuit distinguished *Clapper* by holding that the plaintiffs sufficiently alleged injury-in-fact to establish Article III standing by showing actual financial harm, a reasonable potential for future harm against all the plaintiffs whose personal data was stolen, and an incurred costs from credit-monitoring services.[104] The Seventh Circuit distinguished *Clapper* because that case involved a mere suspicion that the government was intruding on plaintiffs' privacy and personal data, while *Remijas* involved both a substantial risk to plaintiffs

---

[101] *Id.*

[102] *Galaria*, 663 F. App'x at 388-89 (concluding that although defendant Nationwide offered to provide some credit-monitoring services, plaintiffs sufficiently alleged that their harm extended beyond the defendant's one-year offer to provide these services).

[103] *Galaria*, 663 F. App'x at 389; Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015).

[104] *Remijas*, 794 F.3d at 693-96.

whose personal data was already compromised and actual harm to plaintiffs who could show fraudulent charges on their credit cards.[105]

Like the plaintiffs in *Galaria*,[106] the plaintiffs, customers of Neiman Marcus, should not have to wait for hackers to place fraudulent charges on the plaintiffs' credit cards or suffer some other actual harm to their personal or financial security to establish standing.[107] The Seventh Circuit found there was an "objectively reasonable likelihood" that an injury to the plaintiffs would occur following the breach.[108] The court noted its presumption that once a hacker obtains personal information, including credit card information, the hacker plans to use it fraudulently.[109]

The *Remijas* court considered the future economic harm to the plaintiffs when determining standing.[110] The court recognized certain intangible harms, including the plaintiffs' assertion that fraudulent charges and risk of identity theft can continue long after an initial breach.[111] The plaintiffs cited a Government Accountability Office Report which found that "stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data

---

[105] *Id.* at 693.
[106] *Galaria*, 663 F. App'x at 388.
[107] *Remijas*, 794 F.3d at 693 ("[T]he risk that [p]laintiffs' personal data will be misused by the hackers . . . is immediate and very real." (quoting *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (comparing the instant case to *In re* Adobe Sys., Inc. Privacy Litig. and *Clapper*))).
[108] *Id.* at 694 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).
[109] *Id.* at 693 ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities.").
[110] *Id.* at 694.
[111] *Id.* at 693-94.

have been sold or posted on the Web, fraudulent use of that information may continue for years."[112] This suggested that a plaintiff may be at risk for at least a year after their personal data was initially breached.[113]

The court in *Remijas* reiterated the importance of not over-reading *Clapper*, especially where the plaintiffs have already received notice of their personal information being compromised and the defendant does not contest the breach of information.[114] It is also reasonable for a plaintiff-customer, after notification of the breach, to take steps to protect their finances and identity, such as credit-monitoring procedures.[115] Following the analysis in *Galaria*,[116] the Seventh Circuit in *Remijas* considered the fact that Neiman Marcus offered one year of credit-monitoring and identity protection measures in assessing the severity of the plaintiffs' risk of future harm.[117] Notably, the Seventh Circuit considered the actual price of credit-monitoring services in determining a sufficient and concrete injury.[118] The court mentioned that credit-monitoring services come at a price that easily qualifies as a concrete injury, supporting this with an example that Experian offers

---

[112] *Id.* at 694 (citing U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 29 (2007)).
[113] *Remijas*, 794 F.3d at 694.
[114] *Id.* (noting that *Clapper* addressed a speculative harm that may or may not happen to plaintiffs).
[115] *Id.* (stating that an affected customer might think it is necessary to subscribe to a monthly credit-monitoring service).
[116] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388-89 (6th Cir. 2016).
[117] *Remijas*, 794 F.3d at 694.
[118] *Id.*

credit-monitoring services for $4.95 for the first month, and $19.95 monthly thereafter.[119]

Both *Galaria* and *Remijas* represent the idea that when an initial breach takes place, it is reasonable to assume plaintiffs will incur mitigation costs, and that these costs are not merely speculative or based on hypothetical harm when a plaintiffs' information has already been stolen.[120]

C. Comparing Economic and Legal Theories in Assessing Injury

Economic and legal theories tend to yield different ideas of what constitutes a sufficient injury.[121] Legal theories may not recognize certain privacy costs that economic theories recognize.[122] For example, from an economic perspective, harm resulting from a breach of personal data may include costs such as an increased likelihood that the plaintiff's data will be compromised in the future or an increased probability of receiving spam or computer viruses.[123] Economic theory may also consider the effect on market value of a consumer's data after a breach.[124]

If the plaintiff's data is compromised, economic theory recognizes that both actual and possible costs increase the overall expected costs that a plaintiff may

---

[119] *Id.*
[120] *See Galaria*, 663 F. App'x at 389; *Remijas*, 794 F.3d at 694.
[121] Sasha Romanosky and Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1062-63 (2009). *See* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 114-17 (Anupam Chander et al. eds., 2008) (discussing how the law responds to misuse of personal information that leads to concrete injuries, including financial losses and emotional distress).
[122] Romanosky and Acquisti, *supra* note 121, at 1062-63.

[123] *Id.*
[124] *Id.* at 1063.

incur.[125] The law has also recognized this concept of probabilistic harm, but courts have not reached a consensus on whether probabilistic damage is sufficient to establish injury.[126] This lack of consensus may be due, in part, to the failure to consider or determine the actual costs of tangible and intangible damages that a plaintiff may allege after a data-breach.

The ambiguity of possible future harm resulting from a plaintiff's breach of data is typically not sufficient to establish injury-in-fact.[127] However, Justice Breyer's dissenting opinion in *Clapper* suggests that "courts have often found probabilistic injuries sufficient to support standing,"[128] and that "certainty is not, and never has been, the touchstone of standing."[129] Justice Breyer's dissenting opinion should serve as a starting point for analyzing future harms to create standing. Ultimately, courts should incorporate economic theory in determining whether injury-in-fact exists in data-breach cases.

D. Consumer Data Costs

The risk of losing personal information is balanced with the benefit consumers receive in using this personal data for certain transactions. Consumers using their personal data to complete transactions enjoy benefits of convenience and

---

[125] *Id.*
[126] *Id.*; *see* Richard W. Wright, *Actual Causation vs. Probabilistic Linkage: The Bane of Economic Analysis*, 14 J. LEGAL STUD. 435 (1985) (discussing competing theories of tort liability and the actual causation requirement).
[127] *See* Cease, *supra* note 29, at 414-19 (examining the problems posed by data breach lawsuits).
[128] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 435 (2013) (Breyer, J., dissenting) ("[C]ourts have often found probabilistic injuries sufficient to support standing.").
[129] *Id.* at 431 (Breyer, J., dissenting).

easier access to credit and insurance,[130] data customization for interactivity purposes,[131] and personalization – including customized views based on previous purchases.[132]

However, the misuse of this personal information can lead to a wide array of financial losses, both direct and indirect. Personal data can be used for a variety of purposes, including identity theft, fraud, spam marketing or telemarketing, among others.[133] The direct harm resulting from these data-breaches includes financial loss when a hacker uses credit card or bank information to make fraudulent purchases.[134] Identity theft can also take the form of hackers opening fraudulent accounts or using personal information to obtain loans.[135]

After a consumer's personal data is breached, the next reasonable step is for that consumer to protect their personal information, which can be accomplished using a variety of measures.[136] Most commonly, companies will suggest or offer

---

[130] Romanosky & Acquisti, *supra* note 121, at 1063; *see* Nicola Jentzsch, *The Regulation of Financial Privacy: The United States vs. Europe*, ECRI RESEARCH REPORT NO. 5, June 1, 2003 (analyzing the economic effects associated with different privacy regulations); *see* Nicola Jentzsch & Amparo San José Riestra, *Consumer Credit Markets in the United States and Europe*, *in* THE ECON. OF CONSUMER CREDIT 27 (Giuseppe Bertola et al., eds., 2006) (comparing consumer credit markets in various countries).

[131] *See* Robert C. Blattberg, & John Deighton, *Interactive Marketing: Exploiting the Age of Addressability*, 33 SLOAN MGMT. REV. 5, 5 (1991) (discussing the power of today's consumer to shape marketing resources for firms through databases of transactional history).

[132] Alessandro Acquisti & Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MARKETING SCI. 367, 374 (2005).

[133] Solove, *supra* note 121, at 115-16.

[134] *Id.* at 115.

[135] Robert O'Harrow Jr., *Identity Thieves Thrive in the Information Age*, WASH. POST (May 31, 2001), https://www.washingtonpost.com/archive/politics/2001/05/31/identity-thieves-thrive-in-information-age/2d960d5e-ff0a-4bc1-94f3-ace62f44fe78/?utm_term=.9e7a2d4f9fd4.

[136] Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (stating that an affected customer might think it is necessary to subscribe to a monthly credit-monitoring service).

credit-monitoring services.[137] However, companies who offer credit-monitoring or identity theft protection services following a data-breach typically provide their services for only one year.[138] As discussed, this one-year time span is usually insufficient to provide full protection of the data-breach victim.[139]

Victims of data-breaches incur financial loss from purchasing credit-monitoring and other services to protect their financial and personal data.[140] These services include not only purchasing credit-monitoring services, but also less calculable expenses: personal time expended canceling credit cards and opening new ones; changing passwords and usernames or email addresses; calling companies directly to verify information; closing and reopening new banking accounts; reporting to banks; having a credit reporting agency place a fraudulent alert on the plaintiff's account (if the plaintiff's social security number was exposed); placing credit freezes on one's account; inserting new card information into plaintiff's auto-fill program; and changing recurring payment methods.[141]

In addition to these harms, plaintiffs have also alleged suffering loss of rewards points on credit cards and enduring general anxiety that their information

---

[137] Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).
[138] *See id.* (noting that defendant insurance company offered credit-monitoring services for one year following the data breach).
[139] *Id.* at 388-89 (concluding that although defendant Nationwide offered to provide some credit-monitoring services, plaintiffs sufficiently alleged that their harm extended beyond the defendant's one-year offer to provide these services).
[140] Solove, *supra* note 121, at 115-16.
[141] *What Should I Do if I Have Been a Victim of a Data Breach?*, TIME: MONEY (May 26, 2014), http://time.com/money/2791976/data-breach-victim/.

may be compromised in the future to make unauthorized purchases.[142] Consumers may also suffer from discrimination or social stigma as a result of a data-breach.[143] Another example of an indirect consumer cost is when a consumer responds to a breach notification: the consumer must first process the information and then determine the next best steps.[144] This consumer response is a significant cognitive cost and may represent an undue burden on the consumer.[145]

## IV. Proposal

Courts should provide relief for data-breach plaintiffs where personal information has been compromised as a result of a defendant company's lapse, and the plaintiffs have taken reasonable measures to remedy their financial losses from the breach. Courts should provide for relief when there is some level of actual harm to the plaintiffs' personal or financial information, at which point it may be presumed that the purpose of the hack was to make fraudulent charges or commit identity theft.[146] Hackers who steal credit card and other personally identifying information seemingly have one goal in mind: to use that sensitive information

---

[142] *See In re* Hannaford Bros. Co. Consumer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 114 (D. Me. 2009) (explaining examples of collateral consequences, including lost opportunities to earn rewards points, fear of a fraudulent transaction in the future, or other incidental expenses); John Biglow, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943 (2016).

[143] *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELEC. COMMERCE 21 (2004) (analyzing consumers' fears about privacy and security concerns.)

[144] Romanosky & Acquisti*, supra* note 121, at 1066.

[145] *Id.*; *see also* Janine Benner, Beth Givens, & Ed Mierzwinski, *Nowhere to Turn: Victims Speak Out on Identity Theft: A CALPIRG / Privacy Rights Clearinghouse Report* (May 2000), http://www.privacyrights.org/ar/idtheft2000.htm.

[146] *See* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693-94 (7th Cir. 2015) (presuming that the only reason hackers break into a store's database and steal consumers' credit card and other identifying information is to, at some point in the future, make fraudulent charges or commit identity theft).

fraudulently and at the expense of the data-breach plaintiff. In summary, when a court finds that plaintiffs have suffered any level of actual harm to their personal information, courts should grant Article III standing.

On the other hand, when the data-breach plaintiffs' information has been stolen, and the plaintiffs have not yet received fraudulent charges or any other measurable harm to their private information, courts should analyze the probability of future expenses to determine whether the plaintiffs have standing. The issue in these types of cases is whether indirect costs and expenses are sufficient to meet the injury requirement per Article III.

A. Reasonable Indirect Costs may be Quantified

Although future expenses are generally insufficient for standing,[147] the costs that plaintiffs incur to protect themselves from future harm can be quantified in a legally cognizable way. These protective measures should be evaluated on a reasonableness standard—that is, whether the costs the plaintiffs spent to mitigate future harm were reasonable under the circumstances. The harm must also be imminent.[148] This can be evaluated using a number of factors, including an understanding of the seriousness of the breach, which may shed light on whether the plaintiffs' actions were reasonable.

---

[147] Dana Post, *Plaintiffs Alleging Only "Future Harm" Following a Data Breach Continue to Face a High Bar*, I'NT'L ASS'N PRIVACY PROF'LS. (Jan. 28, 2014), https://iapp.org/news/a/plaintiffs-alleging-only-future-harm-following-a-data-breach-continue-to-fa/# (stating that with the exception of a few cases, most courts have dismissed private lawsuits involving data breaches where the plaintiffs have not suffered a concrete injury due to the difficulty of quantifying the harm of a mere data breach).

[148] *See Remijas*, 794 F.3d at 694 (holding that mitigation expenses do not qualify as actual injuries where the harm is not imminent) ("[Plaintiffs] cannot manufacture standing by incurring costs in anticipation of non-imminent harm[.]") (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 402 (2013))).

For example, courts should consider whether the defendant-company has offered or suggested certain services to protect plaintiffs' financial security. Courts should follow the reasoning adopted by the Seventh Circuit Court of Appeals in *Remijas*, where the court considered the fact that defendant, Neiman Marcus, offered one year of credit-monitoring and identity-protection measures to reflect the severity of the plaintiffs' risk of future harm.[149] After a plaintiff has received notice of the breach and the defendant suggests credit-monitoring services, it is reasonable for a plaintiff to incur costs to protect their financial security. The amount a plaintiff spends on these protective services should not be excessive; they should follow the same guidelines and suggestions provided by the defendant upon notification of the breach. A court should not recognize excessive expenditures that go well beyond what would suffice as reasonable protections against fraud. The security measures should be viewed in light of the surrounding circumstances, including the amount of information lost, the sensitivity and complexity of that information, and the cost of available remedies to protect against data fraud.

A data-breach plaintiff may decide to purchase credit-monitoring services for one year, which is a typical timeframe for actual harm to occur following a data-breach.[150] However, it is possible for plaintiffs to show that harm is still occurring after one year. While expenses may continue after the one-year mark, plaintiffs should be able to avoid the continued harm by changing bank accounts, creating

---

[149] *Id.*

[150] *Id.* at 690 (stating 9,200 customers who alleged actual fraud all experienced it within six months of the breach).

new passwords, and closing any compromised financial accounts within that first year. Plaintiffs should be able to recover for the expenses and time spent to mitigate the future harm, and courts should consider credit-monitoring services beyond one year to be reasonable depending on the severity of the data-breach.

Damages based on an increased risk of identity theft alone are generally too speculative for a court to consider as sufficient injury. Anticipated harm that is too far-removed from a data-breach should not be considered sufficient injury alone. However, data-breach plaintiffs should not be forced to wait and see if an actual injury will occur once their personal information has been accessed. In some cases, this may cause emotional distress and create a stressful "waiting game" of sorts where the plaintiff is continually checking their accounts to make sure their information has not been compromised.

To prevent this unnecessary waiting game burden, plaintiffs should take measures to protect their information after first notification of a breach. If courts do not recognize these mitigation costs to qualify as sufficient injury and require plaintiffs to wait for an actual injury to occur, then plaintiffs will likely have no recourse in this situation. If the plaintiffs incur costs to mitigating potential harm, then the actual harm is much less likely to occur in the long run, which ultimately leaves the plaintiffs with more out-of-pocket expenses and a lesser chance of obtaining relief in court. Another issue with the wait-and-see approach is that the damage is more difficult to prove after significant time passes following a data-breach.

B. Costs of Monitoring Services Should be Recoverable

Money spent on monitoring services following a breach should be recoverable. Again, this should be determined on a reasonableness standard, using a one-year mark for credit-monitoring services as a general guideline. Generally, the time and money spent to monitor financial and personal information should go hand-in-hand with the costs incurred from changing accounts and passwords. These steps should be taken as essential responsibilities of a plaintiff, and as such, the plaintiff should be compensated for those expenditures. These expenditures are admittedly quite small, with credit and identity theft monitoring services ranging from about $120 to $200 per year.[151] However, allowing for recovery of monitoring services provides plaintiffs with an invaluable peace of mind to know they will not be burdened by these expenses.

It is reasonable for plaintiffs, after receiving a notification of a breach of their data, to invest in monitoring services and spend time and money creating and cancelling bank accounts.[152] Customers should have a reasonable belief that the data stolen could result in harm to their personal or financial security. For example, a plaintiff who has only given out his or her email to a defendant-company may have less of a belief that the email will be used against the plaintiff compared to a plaintiff who has his or her credit card or social security information stolen.

---

[151] *Should I Pay for Credit Monitoring?*, TIME: MONEY, www.time.com/money/collection-post/2791979/should-i-pay-for-credit-monitoring/. (last visited Feb. 26, 2019).

[152] *Remijas*, 794 F.3d at 694 (stating that an affected customer might think it is necessary to subscribe to a monthly credit-monitoring service).

Courts should also consider the number of accounts affected in the breach to determine whether the monitoring costs were reasonable.[153] While data-breach-notification laws differ across states, in general, if a company is legally required to send out a data-breach notification, the likelihood of the plaintiff's personal information being fraudulently used is substantial.[154]

C. Indirect Costs Should be Compensated

Time spent to cancel bank accounts, order new credit cards, change passwords, place credit freezes on accounts, call companies directly to verify fraudulent charges, and other communication with banks and financial services should be considered compensable, indirect costs that qualify as a sufficient injury. These indirect costs should be reasonable and distinguished from mere conjectural future harm.

The amount of time and money spent to protect against future fraud ranges depending on the circumstances.[155] Over half of identity victims resolved any problems associated with the data-breach within a day or less; about nine percent

---

[153] *See* Megan Dowty, Note, *Life is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 705 (2017) (explaining that it may not be possible for companies to know the exact number of consumers affected by any given data breach).

[154] Security Breach Notification Laws, NAT'L CONF. OF STATE LEGISLATURES (Feb. 24, 2016), www.ncsl.org/research/telecommunications-and-information-technology/security-breachnotification-laws.aspx; *see also id.* (providing an overview of state data-breach-notification requirements).

[155] Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html (reporting the experiences of data breach victims, including one woman who spent nine months trying to convince the IRS that her identity was stolen; she then reported the identity theft to the police, filed an affidavit, contacted the credit bureaus, and then contacted the Ohio government).

spent over a month trying to sort out their information.[156] In general, encouraging victims of data-breaches and identity theft to incur these indirect costs will result in fewer breaches and fraudulent charges overall. Thus, courts should promote a mutually beneficial public policy that allows data-breach plaintiffs to recover for the reasonable costs incurred to avert the threatened harm of identity theft or fraudulent charges.

## V. Conclusion

Courts must face the stark reality that data-breaches have joined the ranks of taxes and death as certainties. Companies can take regulatory steps to prevent data-breaches from happening—but as long as we're living in a digital world, hackers will continue to develop new ways to hack information systems. While legislatures can put regulations in place as preventative measures, the judiciary needs a uniform system for relief when a data-breach inevitably occurs.

From an economic perspective, the difference between actual and potential injury is a measure of probability. Courts should recognize that both actual and potential injuries increase a plaintiff's expected costs from a data-breach. Certain tangible and intangible costs are admittedly difficult to measure, but the costs incurred following a data-breach to avert potential future harm should be evaluated from a reasonableness standpoint in determining whether a plaintiff has sufficient

[156] BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ248991, VICTIMS OF IDENTITY THEFT, 2014 (2015), www.bjs.gov/content/pub/pdf/vit14_sum.pdf. In addition, identity theft victims whose accounts were compromised were more likely to resolve any financial issues within twenty-four hours than victims who suffered from multiple types of identity theft. *Id.*

standing to bring a data-breach claim. Private lawsuits without a concrete injury should not immediately be dismissed. Instead, courts should consider the impact of data-breaches and the plaintiffs' incurred costs to avoid future harm in determining Article III standing.