Boston College Law Review

Volume 59
Issue 9 *Electronic Supplement*

Article 26

5-22-2018

No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions

Brandon Ferrick
Boston College Law School, brandon.ferrick@bc.edu

NO HARM, NO FOUL: THE FOURTH CIRCUIT STRUGGLES WITH THE "INJURY-IN-FACT" REQUIREMENT TO ARTICLE III STANDING IN DATA BREACH CLASS ACTIONS

Abstract: On February 6, 2017, in *Beck v. McDonald*, the United States Court of Appeals for the Fourth Circuit held that the increased risk of future identity theft created by two data breaches was too speculative to constitute an injury-in-fact for the purposes of Article III standing. The court surveyed the split between its sister circuits and determined that, without allegations that a thief deliberately targeted information, misused, or attempted to misuse that personal information, the risk of identity theft was not sufficiently high so as to meet the injury-in-fact requirement of Article III standing. This Comment examines the Fourth Circuit's holding and argues that the deepening split among circuits leaves plaintiffs uncertain about how to adequately plead injury-in-fact.

INTRODUCTION

Following a data breach, victims that bring a lawsuit typically claim three types of injuries: (1) actual financial harm, (2) actual identity theft or misuse of personal information without financial harm, and (3) an increased risk of future identity theft or other misuse.[1] Courts regularly find standing

[1] Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, 16 CLASS ACTION LITIG. REP. (BNA) 1054, 1055 (Sept. 25, 2017). "A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion." Margaret Rouse, *Data Breach*, TECHTARGET (Dec. 2017), http://searchsecurity.techtarget.com/definition/data-breach [https://perma.cc/VC8W-FEVA]; *see also* William Roberds & Stacey L. Schreft, *Data Breaches and Identity Theft*, 56 J. MONETARY ECON. 918, 919–20 (2009) (describing the prevalence of data breaches). Data breaches may involve the theft of personal health information, personally identifiable information, trade secrets, or intellectual property. *See* Fram et al., *supra* at 1055 (discussing lawsuits following "hacking, point-of-sale attacks, [and] hardware theft"). Irrespective of how much money companies spend on cybersecurity defense, data breaches continue to occur and millions of individuals have their personal information stolen, especially in the cybersecurity context. *See* Selena Larson, *Why Hacks Like Equifax Will Keep Happening*, CNN TECH (Sept. 29, 2017), http://money.cnn.com/2017/09/29/technology/business/equifax-hack-2017-cyberattacks/index.html [https://perma.cc/Q3W3-3B9Q] (discussing the recent Equifax hack and other targeted data breaches, noting that, in the first half of 2017 alone, "almost 2 billion records were lost or stolen globally"); Michael Riley et al., *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros [https://perma.cc/7TCC-TVRG] (discussing the recent Equifax hack of 143 million customers' personal information). Data breaches are particularly frustrating for victims because they often cannot find the perpetrator who actually stole their information. *See* Riley et al., *supra* (commenting on how victims

where a plaintiff alleges actual financial harm or misuse of personal information.[2] Courts struggle to find standing, however, where a plaintiff merely alleges an increased risk of future harm as a result of a data breach.[3] That struggle is disconcerting to victims because an increased risk of future identity theft is the most commonly alleged injury in lawsuits following data breaches.[4] This Comment discusses the current split among the circuits

---

don't know who stole their personal information). Victims of data breaches are left in a constant state of anxiety that their personal information will be manipulated and fraudulently used against them. *Id.* Thus, potential plaintiffs have no recourse but to sue the companies that they trusted with their personal information. *See* Nick Beatty, Note, *Standing Room Only: Solving the Injury-in-Fact Problem for Data Breach Plaintiffs*, 2016 BYU L. REV. 1289, 1290 (discussing the typical data breach class action, in which plaintiffs sue their once-trusted companies for "negligence in protecting [their] financial information"); *see, e.g.*, Beck *v.* McDonald, 848 F.3d 262, 267 (4th Cir. 2017) (detailing plaintiffs' suit against a hospital for failure to take adequate precautions to keep their personal information secure in wake of data breach). Being forced to sue a once-trusted company is potentially the most frustrating part of a data breach for victims because there often was an expectation that the defendant companies would keep that personal information safe and secure. *See* Pat Regnier & Suzanne Woolley, *Thank You for Calling Equifax. Your Business Is Not Important to Us*, BLOOMBERG BUSINESSWEEK (Sept. 14, 2017), https://www.bloomberg.com/news/features/2017-09-14/thank-you-for-calling-equifax-your-business-is-not-important-to-us [https://perma.cc/5UZ7-LC7C] (discussing the inherent anxiety victims of data breaches face, commenting, "you shouldn't need to do a damn thing to keep your credit information safe"). Data breaches can also arise even where individuals did not voluntarily enter into a relationship with the hacked company, thus causing further headaches for data breach victims. *See id.* (discussing the frustration surrounding the 2017 Equifax, Inc. hack, noting "what makes the situation especially awful is that you never had much choice about entering into a relationship with Equifax").

[2] WHAT'S "NEW" IN CYBERSECURITY (2017): LITIGATION AND ENFORCEMENT ACTIONS, CU*ANSWERS, 18–20 (May 24, 2017), http://nascus.org/Cyber17/handouts/Sickels%20pt2%20whats%20new.pdf [https://perma.cc/3C24-Z4VX] [hereinafter WHAT'S "NEW" IN CYBERSECURITY]; Fram et al., *supra* note 1, at 1055; J. Thomas Richie, *Data Breach Class Actions*, A.B.A. BUS. LITIG. COMMITTEE NEWSL., Winter 2015, at 1, 10–11; *see, e.g.*, *In re* Target Corp. Customer Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding standing "sufficient at [the] pleading stage" where customers whose credit card information was stolen alleged unlawful charges, inability to pay bills, and new, unauthorized credit card fees); Tierney v. Advocate Health & Hosps. Corp., No. 13 CV 6237, 2014 WL 5783333, at *2 (N.D. Ill. Sept. 4, 2014) (finding standing for named plaintiffs who alleged fraudulent account activity, but concluding the majority of plaintiffs did not have standing where they only alleged an increased risk of identity theft), *aff'd on other grounds*, 797 F.3d 449 (7th Cir. 2015).

[3] *See* Megan Dowty, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686, 688 (2017) (noting that "courts' rulings vary the most" in the injury-in-fact context for data breach class actions, and that plaintiffs mainly try to "allege injury through increased risk of identity theft or fraud . . . ."); Fram et al., *supra* note 1, at 1057 (discussing the differences in precedent among federal courts).

[4] Fram et al., *supra* note 1, at 1057; *see, e.g.*, Attias v. Carefirst, Inc., 865 F.3d 620, 623 (D.C. Cir. 2017) (finding standing where plaintiffs alleged increased risk of injury following cyber hack); *Beck*, 848 F.3d at 267–68, 275 (declining to find standing where plaintiffs alleged increased risk of identity theft following theft of a laptop and pathology reports from hospital); Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016) (finding standing where plaintiffs alleged increased risk of identity theft following hack on Nationwide's computer network); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 965, 967 (7th Cir. 2016) (finding standing where plaintiffs alleged increased risk of identity theft following hack of credit card in-

concerning potential-future-injury theories of standing and further details the current lack of certainty regarding what constitutes injury-in-fact.[5] Part I of this Comment discusses the background of standing in federal courts, the reasoning applied to standing considerations by other courts in data breach class action suits, and the procedural history of the recent Fourth Circuit case, *Beck v. McDonald*.[6] Part II analyzes the Fourth Circuit's discussion and ruling in *Beck*.[7] Part III explains that, in the midst of the current circuit split, plaintiffs are left uncertain regarding how to adequately plead injury-in-fact in data breach class actions.[8]

I. FACTUAL AND LEGAL BACKGROUND OF *BECK V. MCDONALD*

In federal court, before plaintiffs can proceed to argue the merits of their cases, they must first prove they have a cognizable stake in the litigation: this is considered having standing.[9] To sufficiently prove that a plaintiff has standing, that plaintiff must demonstrate that they have suffered an injury.[10] In the data breach context, there is currently no consensus regarding whether merely having personal information stolen by a third party and, as a result, being at an increased risk of identity theft, is sufficient to establish standing.[11] Some courts have ruled that an increased risk of identity theft, alone, is a sufficient injury to confer standing.[12]Other courts have been reluctant to take that position and instead require some evidence—beyond the mere occurrence of a data breach—that financial harm is cer-

---

formation from P.F. Chang's); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015) (finding standing where plaintiffs alleged increased risk of identity theft following hack of Neiman Marcus's customers' credit card numbers).

[5] *See infra* notes 9–110 and accompanying text.

[6] *See infra* notes 9–65 and accompanying text.

[7] *See infra* notes 66–85 and accompanying text.

[8] *See infra* notes 86–110 and accompanying text.

[9] Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 882 (1983). Standing, put simply, is having a stake in the litigation. *Id.*

[10] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (citing Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)); *see* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 475, (1982) ("The exercise of judicial power, which can so profoundly affect the lives, liberty, and property of those to whom it extends, is . . . restricted to litigants who can show 'injury in fact' resulting from the action which they seek to have the court adjudicate.").

[11] *Compare Attias*, 865 F.3d at 626 (finding standing where plaintiffs only alleged increased risk of future identity theft without any attempted or actual misuse of personal information), *with Beck*, 848 F.3d at 275 (finding that plaintiffs lacked standing where they alleged only an increased risk of identity theft without pleading actual or attempted misuse of personal information).

[12] *See, e.g.*, *Attias*, 865 F.3d at 629 (noting that a substantial risk of harm "exists . . . . simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken").

tainly impending to recognize a plaintiff's standing.[13] Section A of this Part provides a brief introduction to federal standing and an overview of circuit courts' struggle for homogeneity in data breach class actions.[14] Section B discusses the procedural history of *Beck*, a recent Fourth Circuit case involving allegations of violations of the Privacy Act and the Administrative Procedure Act ("APA") resulting from two data breaches.[15]

A. Legal Background

Federal courts have the constitutional authority to exercise the judicial power of the United States.[16] Courts are limited to hearing only cases and controversies in the exercise that power in an effort to maintain a balance of power between the branches of government.[17] In order for a matter to meet the cases or controversies requirement, plaintiffs "must establish that they have standing to sue."[18]

Standing is a threshold requirement that determines whether a court is entitled to decide the merits of a dispute.[19] Standing ensures that the federal courts do not overstep their proper judicial authority and waste judicial resources by hearing frivolous claims, but rather focus on resolving actual disputes between adversaries.[20] Relaxing the standing requirement would

---

[13] *See, e.g.*, *Beck*, 848 F.3d at 274 (noting that plaintiffs "uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor . . . that the thief stole the laptop with the intent to steal their private information").

[14] *See infra* notes 16–41 and accompanying text.

[15] *See infra* notes 42–65 and accompanying text. This Comment only discusses the Fourth Circuit's analysis of plaintiffs' claims under the Privacy Act, not under the APA. *Id.*

[16] U.S. CONST. art. III, §§ 1–2

[17] *See* Warth v. Seldin, 422 U.S. 490, 498–501 (1975) (discussing the purpose of standing, noting that standing is concerned with properly limiting the role of courts in a democracy); Hayburn's Case, 2 U.S. (2 Dall.) 409, 419 n.† (1792) ("[B]y the Constitution of the United States, the government thereof is divided into three distinct and independent branches, and . . . it is the duty of each to abstain from, and to oppose, encroachments on either."); *see also* Scalia, *supra* note 9, at 882 (discussing the importance of Article III standing as a check on judicial power).

[18] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560, (1992)).

[19] *Lujan*, 504 U.S. at 560.

[20] *Id.* at 598 n.4 (noting the purpose of standing is to resolve "genuine controversies between adverse parties"); *see* Marbury v. Madison, 5 U.S. (1 Cranch) 137, 170 (1803) ("The province of the court is, solely, to decide on the rights of individuals."). In the words of the late Justice Antonin Scalia, the purpose of standing is to have federal courts adjudicate cases where the parties can adequately answer the question, "What's it to you?" Scalia, *supra* note 9, at 882 (discussing the importance of Article III standing as a check on judicial power). Standing also serves other goals such as ensuring adverse litigants and promoting democracy. *See* Heather Elliot, *The Functions of Standing*, 61 STAN. L. REV. 459, 465–501 (2008) (discussing other justifications for standing).

inappropriately expand judicial power.[21] Thus, a federal court's inquiry into standing must be laborious and thorough in every case in order to keep the courts within the bounds of its judicial role.[22]

The Supreme Court has declared three "irreducible constitutional minim[a]" that plaintiffs must allege to establish standing: "(1) an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[23] To establish injury-in-fact, a plaintiff must demonstrate that he or she suffered an "actual or imminent" harm that is "concrete and particularized."[24]

In 2013, in *Clapper v. Amnesty International USA*, the Supreme Court set forth the current understanding of the actual-or-imminent component of injury-in-fact.[25] In *Clapper*, the plaintiffs challenged the Foreign Intelligence Surveillance Act ("FISA") because they were concerned their client-communications were being unlawfully intercepted and surveilled by the

---

[21] *Lujan*, 504 U.S. at 559–60. The concept of standing is founded on the bedrock principle of separation of powers. *See Spokeo*, 136 S. Ct. at 1547 ("[Standing] developed in our case law to ensure that federal courts do not exceed their authority as it has been traditionally understood.").

[22] *Spokeo, Inc.*, 136 S. Ct. at 1547 (citing *Warth*, 422 U.S. at 498); *see* Jerett Yan, *Standing as a Limitation on Judicial Review of Agency Action*, 39 ECOLOGY L.Q. 593, 596 (2012) (explaining that one of the functions of Article III standing is to maintain a separation of powers, noting that, by "limiting the power of the judiciary . . . decisions are made by the accountable political branches rather than the unaccountable judiciary"). A rigorous standing inquiry ensures that the judiciary does not step into the realm of policymaking and maintains adjudicative authority over violations of rights. *Id.* at 596–97.

[23] *Spokeo, Inc*., 136 S. Ct. at 1547 (citing *Lujan*, 504 U.S. at 560); *see also* Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009) (stating, plaintiff "bears the burden of showing that [they have] standing"); Fair Elections Ohio v. Husted, 770 F.3d 456, 459 (6th Cir. 2014) ("Each element of standing 'must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at successive stages of the litigation.'"). The requirements for standing do not change when plaintiffs bring class actions as opposed to individual actions. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 634 (3d Cir. 2017); *see* Lewis v. Casey, 518 U.S. 343, 357 (1996) ("[N]amed plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'"); O'Shea v. Littleton, 414 U.S. 488, 494 (1974) ("[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class."); *see also* Neale v. Volvo Cars of N. Am., LLC, 794 F.3d 353, 362 (3d Cir. 2015) ("[T]he 'cases or controversies' requirement is satisfied so long as a class representative has standing, whether in the context of a settlement or litigation class.").

[24] *Spokeo*, 136 S. Ct. at 1547 (quoting *Lujan*, 504 U.S. at 560). This requirement ensures that a plaintiff has "a personal stake" in the litigation, and it aims to ensure that the plaintiff bringing the suit is the proper representative of the grievance. *Attias*, 865 F.3d at 626. Courts consistently find that actual identity theft amounts to a "concrete and particularized injury." *Id.* at 627. The issue that courts are split over, at least at the pleading stage, is whether allegations of a future risk of identity theft can confer standing. *See id.*

[25] *Clapper*, 568 U.S. at 409.

government.[26] The Supreme Court decided that the plaintiffs did not have standing to challenge FISA because they could not establish that their communications with their clients were intercepted or that interception by the government was imminent.[27]

The Court acknowledged that the threat of injuries can satisfy Article III's standing requirement so long as the threat is imminent, not merely possible, or objectively reasonable.[28] The Court maintained that a threatened or future injury satisfied the imminence requirement if it is "certainly impending."[29] The Court was careful to point out that "certainly" would not require absolute certainty, and that standing could also be established by showing that a plaintiff reasonably incurred costs to mitigate or avoid a substantial risk of harm.[30] Consequently, speculative injuries—injuries that require courts to connect chains of events together to reach—are insufficient to confer stand-

---

[26] *Id.* at 406–07. FISA is a United States federal law that provides the guidelines and procedures for the surveillance of foreign intelligence. 50 U.S.C.A. §§ 1881, 1881(a)–(g) (West 2018).

[27] *Clapper*, 568 U.S. at 410–11. The plaintiffs only alleged that they suspected that such interceptions might have occurred but could not establish that they had in fact happened or were sufficiently likely to happen in the future. *Id.* The Supreme Court found that plaintiffs could not prove that they had any actual knowledge of the government's surveillance practices. *Id.* Rather, the plaintiffs merely surmised about the intentions and plans of the government to intercept their clients' communications. *Id.*

[28] *Id.* at 409. Indeed, the Court recently reaffirmed that "the real risk of harm [can] satisfy" Article III's standing requirements. *Spokeo*, 136 S. Ct. at 1549 (citing *Clapper*, 568 U.S. 398). Scholars have also pointed out that the Court has not been clear as to whether imminence refers to a time-based concept, a "probabilistic concept," or both. *See* Evan Tsen Lee & Josephine Mason Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 179–80 (2012) (discussing the Supreme Court's lack of clarity in applying the imminence element of injury-in-fact); *see also, e.g.*, *Lujan*, 504 U.S. at 563, 564 (finding lack of imminence where the Court's concern appeared to be that the injury was not precipitating immediately); Los Angeles v. Lyons, 461 U.S. 95, 102 (1983) (finding lack of imminence where injury was too "conjectural," implying that the probability of the occurrence of harm was insufficient).

[29] *Clapper*, 568 U.S. at 409.

[30] *Id.* at 414 n.5 ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.") (citing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 152–54 (2010)). There is debate amongst scholars as to whether there truly exists a "substantial harm" test, or whether it was merely included in *Clapper* as a way to secure Justice Kennedy's vote for the majority. Nicholas Green, *Standing in the Future: The Case for a Substantial Risk Theory of "Injury in Fact" in Consumer Data Breach Class Actions*, 58 B.C. L. REV. 287, 302 (2017). The Supreme Court in *Spokeo* acknowledged that *Clapper* permits a substantial risk theory of injury, but some circuit courts are still reluctant to apply anything other than the certainly impending standard. *Compare Spokeo*, 136 S. Ct. at 1549 (acknowledging the viability of a substantial risk theory of injury in fact), *with* Blum v. Holder, 744 F.3d 790, 797 (1st Cir. 2014) (applying *Clapper*'s certainly impending standard, discussing the ambiguity in *Clapper*). To the extent the standard exists, the *Beck* court decided to apply it and determined that the plaintiffs could not establish standing to sue. *See Beck*, 848 F.3d at 275. The Supreme Court has since clarified, in *Susan B. Anthony List v. Driehaus*, that a plaintiff can establish standing by satisfying either the "certainly impending" test or the "substantial risk" test. 134 S. Ct. 2334, 2341 (2014).

ing.[31] The Court refused to find standing based on speculation about the decisions of third parties, and found the plaintiffs' alleged injury too abstract to be certainly impending.[32]

In data breach cases, the injury-in-fact element is often the most contentious.[33] In that context, courts struggle to answer whether identity theft is certainly impending following a data breach.[34] Most district courts have held that identity theft is not certainly impending after a data breach absent facts beyond the mere occurrence of the breach.[35] Several circuit courts have held the same.[36] Recently, however, a few circuit courts have found

---

[31] *See* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (finding that "allegations of possible future injury do not satisfy the requirements of Art. III" and that only "certainly impending" injuries "constitute injury-in-fact"); *see also Clapper*, 568 U.S. at 410 (finding plaintiffs theory of future injury too speculative to confer standing).

[32] *Clapper*, 568 U.S. at 414.

[33] *See* Beatty, *supra* note 1, at 1296 (noting the problems data breach plaintiffs face in trying to plead injury-in-fact, describing courts' hesitations to find injury-in-fact where plaintiffs fail to allege any economic loss); *see also Spokeo*, 136 S. Ct. at 1547 (citing, Steel Co. v. Citizens for Better Env't, 523 U.S. 83, 103 (1998) (noting that the injury-in-fact component is the "[f]irst and foremost" element of standing).

[34] Green*, supra* note 30, at 315 (noting a diverging view on *Clapper*'s standing requirements in the federal circuits); Richie, *supra* note 2, at 10 (examining *Clapper*'s effect on data breach litigation, noting that both before and after *Clapper*, courts split on finding standing for increased risk of future identity theft). In the class action context, the standing requirements are the same as they are for individual plaintiffs. *See In re Horizon* 846 F.3d at 634 ("'[N]amed plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'") (citing *Lewis*, 518 U.S. at 357).

[35] Fram et al., *supra* note 1, at 1057; *see, e.g.*, *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958 (D. Nev. 2015) (holding plaintiffs' alleged risk of identity theft not sufficiently impending where plaintiffs failed to allege any "irregularity whatsoever" concerning their personal information); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015) (finding lack of cognizable injury where class action plaintiffs failed to allege actual identity theft, noting "[t]heir credit information and bank accounts [looked] the same . . . as they did prior to [the] data breach"); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C 2014) (holding that only plaintiffs who alleged actual or attempted misuse of personal data had standing).

[36] *See, e.g.*, *In re Horizon*, 846 F.3d at 639 & n.19 (finding that the plaintiffs alleged a "material risk of harm" where two unencrypted laptops were stolen containing "highly personal" information, where it appeared the laptops were targeted for the personal information contained on them, and at least one named plaintiff alleged he had already been a victim of identity theft as a result of the breach); Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 & n.1 (11th Cir. 2012) (finding that the plaintiff health care members' increased risk of future identity theft was sufficient to confer standing in case of first impression where plaintiffs had alleged actual identity theft, but court refusing to address whether "speculative identity theft" would be sufficient to confer standing); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (refusing to find standing where plaintiff failed to identify "any incident in which her data has ever been accessed by an unauthorized person," noting that, in cases where circuits that have found standing, plaintiffs all alleged actual misuse).

standing based solely on the increased risk of identity theft, without allegations of actual or attempted misuse of information.[37]

The First and Third Circuits have declined to find standing based on an increased risk of identity theft absent corresponding allegations of actual or attempted access or misuse of personal information.[38] The Sixth, Seventh, Ninth, and D.C. Circuits, however, have recognized standing based solely on an increased risk of future identity theft.[39] Most of the cases where the Sixth, Seventh, Ninth, and D.C. Circuits found standing involved conduct deliberately targeting personal information or attempts to use that information for nefarious purposes.[40] Moreover, at least one case in both the Seventh and

---

[37] *See, e.g.*, *Attias*, 865 F.3d at 620, 629 (finding standing based on the increased risk of identity theft following a data breach, holding, "[a] substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken").

[38] *See In re Horizon*, 846 F.3d at 639 & n.19 (finding that the plaintiffs alleged a "material risk of harm" where two unencrypted laptops were stolen containing "highly personal" information, where it appeared the laptops were targeted for the personal information contained on them, and at least one named plaintiff alleged he had already been a victim of identity theft as a result of the breach); *Katz*, 672 F.3d at 80 (refusing to find standing where plaintiff failed to identify "any incident in which her data has ever been accessed by an unauthorized person," noting that, in cases where circuits that have found standing, plaintiffs all alleged actual misuse); Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) (finding a failure to allege injury-in-fact where "appellants have alleged no misuse, and therefore, no injury," noting that "no identifiable taking occurred; all that is known is that a firewall was penetrated[,]" and that there was "no evidence" that the hack was "intentional or malicious"); *see also* Beatty, *supra* note 1 (discussing that, in order to find standing, courts require that plaintiffs show more than merely that their data had been stolen, and must bring forth allegations and evidence of misuse, and economic damages).

[39] *See Attias*, 865 F.3d at 629 (recognizing and applying the substantial-risk standard to find that the plaintiffs met their burden, noting "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *P.F. Chang's China Bistro, Inc.*, 819 F.3d at 967 (recognizing the imminence of future identity theft where customers' credit card data was stolen from restaurant in a hack); *Galaria*, 663 F. App'x at 388 ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in [the p]laintiffs' complaint . . . . Thus, although it might not be 'literally certain' that [p]laintiffs data will be misused, there is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable."); *Remijas*, 794 F.3d at 692, 693–94 (recognizing and applying both the certainly-impending standard and the substantial-risk standard to find plaintiffs met their burden where hackers attacked Neiman Marcus with malware to steal credit card numbers, because "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities"); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (noting that the plaintiff employees' increased risk of future identity theft theory was a "credible threat of harm" for Article III purposes after the theft of a laptop containing unencrypted names, addresses, and social security numbers of 97,000 employees); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632, 634 (7th Cir. 2007) (banking services applicants' increased risk of harm theory satisfied standing requirements after "sophisticated, intentional and malicious" security breach of bank website compromised their personal information).

[40] *See Galaria*, 663 F. App'x at 388 (finding implicitly that the data breach was targeted at personal information); *Remijas*, 794 F.3d at 693–94 (finding that hackers targeted Neiman Marcus with malicious software); *Krottner*, 628 F.3d at 1142 (finding it sufficient to confer standing that a

Ninth Circuits involved at least one allegation of misuse or access of personal information by the thief.[41]

B. Factual Background

In *Beck v. McDonald*, two data breaches at the William Jennings Bryan Dorn Veterans Affairs Medical Center ("Dorn VAMC") in Columbia, South Carolina compromised the personal information of approximately 9,400 veterans.[42] Following the breaches, two classes of plaintiffs brought suits against Dorn VAMC officials, and the Secretary of Veteran Affairs for violations of the Privacy Act and the APA, and various common law claims.[43] In both cases, the plaintiffs sought to establish standing by contending that they suffered harm from the increased risk of, and cost required to prevent, future identity theft.[44] The United States District Court for the District of South Carolina dismissed both actions for lack of subject-matter jurisdiction, holding that the plaintiffs had failed to allege a non-speculative, imminent injury-in-fact for purposes of Article III standing.[45]

The first breach involved the misplacement or theft of a laptop in February 2013.[46] The laptop held the unprotected private information of roughly 7,400 patients.[47] Following the loss of the laptop, Dorn VAMC offered all the potential victims one year of free credit monitoring.[48] At the time of the court's decision in *Beck*, the laptop had not been recovered.[49]

---

thief targeted a laptop containing encrypted personal information); *Pisciotta*, 499 F.3d at 632 (finding hackers acted "intentional[ly]" and "malicious[ly]").

[41] *See Remijas*, 794 F.3d at 693–94 (noting that the plaintiffs are "careful to say that only 9.200 [credit] cards have experiences fraudulent charges *so far*"); *Krottner*, 628 F.3d at 1142 (noting that one plaintiffs alleged actual misuse of personal information). The court, in support of its reasoning, distinguished *Remijas* and other data breach cases from *Clapper*, finding that, unlike the plaintiffs in *Clapper*, the data breach victims did not have to "speculate as to whether [their] information ha[d] been stolen and what information was taken," the plaintiffs were already experiencing fraudulent charges on their credit cards and subsequently alleged that more were yet to come. *Remijas*, 794 F.3d at 693. In contrast, the *Clapper* plaintiffs could only speculate as to whether their communications would be acquired. *Clapper*, 568 U.S. at 411; *Remijas*, 794 F.3d at 693.

[42] *Beck*, 848 F.3d at 266. The breaches affected approximately 7,400 veterans in the first breach and approximately 2,000 in the second. *Id.*

[43] *Id.* at 266–67. This Comment does not discuss the APA or common law claims. See *infra* notes 44–110 and accompanying text.

[44] *Beck*, 848 F.3d at 267, 268.

[45] *Id.* at 268–69.

[46] *Id.* at 267. Although an internal investigation by Dorn VAMC determined the laptop was likely stolen, the court declined to make a finding on that issue. *Id.* at 275.

[47] *Id.* at 275.

[48] *Id.* In addition, Dorn VAMC conducted an internal investigation of the theft, concluding that the laptop was likely to have been stolen and that the Dorn VAMC failed to follow its own policies for securing patient information on laptops. *Id.*

[49] *Id.*

The second breach was uncovered in July, 2014 when Dorn VAMC discovered that four boxes of pathology reports had been misplaced or taken.[50] The boxes contained the information of roughly 2,000 patients, including their names, social security numbers, and medical histories.[51] Just as it had after the first breach, Dorn VAMC offered one year of free credit monitoring to all potential victims.[52] Similarly, at the time of the *Beck* decision, the boxes had not been found.[53]

Following the first breach, named plaintiffs Richard Beck and Lakreshia Jeffrey (the "*Beck* plaintiffs") sued on behalf of a putative class of roughly 7,400 victims whose information was contained on the laptop.[54] The *Beck* plaintiffs sought declaratory relief and monetary damages under the Privacy Act, alleging that the defendants' failures wasted their time and money, embarrassed them, and increased their risk of identity theft.[55] The *Beck* plaintiffs also sought an injunction under the APA ordering the VA to secure, and then destroy, the poorly kept records remaining in Dorn VAMC's hands.[56]

After the defendants moved for summary judgment, the United States District Court for the District of South Carolina dismissed the case for lack of subject-matter jurisdiction, holding that the *Beck* plaintiffs lacked standing under the Privacy Act because they failed to show that identity theft was imminent.[57] Citing *Clapper*, the district court found that the risk of harm from future identity theft was theoretical, not imminent, because it would only occur if the court made assumptions about the actions of third parties.[58] The district court further determined that the plaintiffs lacked standing because they failed to establish a substantial risk of harm.[59] Additionally, the district

---

[50] *Id.* at 268.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.* at 267.

[55] *Id.* (alleging that "the 'Defendants' failures' and 'violations' of the Privacy Act 'caused Plaintiffs . . . embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information'")

[56] *Id.* The *Beck* plaintiffs also brought separate common-law negligence claims. *Id.* The district court granted the Dorn VAMC's motion to dismiss for lack of subject-matter jurisdiction or, in the alternative, for failure to state a claim as to the common-law negligence claims, and declined to dismiss the Privacy Act and APA claims at the pleadings stage. *Id.*

[57] *Id.* at 267–68 (finding that the plaintiffs had "not submitted evidence sufficient to create a genuine issue of material fact as to whether they face a 'certainly impending' risk of identity theft").

[58] *Id.* at 268 (noting that plaintiffs alleged harm was "contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendants").

[59] *Id.* ("The plaintiffs' calculations that 33% of those affected by the laptop theft would have their identities stolen and that all affected would be 9.5 times more likely to experience identity theft 'di[d] not suffice to show a substantial risk of identity theft.'").

court rejected the *Beck* plaintiffs' theory that paying to monitor their credit scores amounted to an injury because the underlying risk of harm was too speculative.[60]

While the *Beck* class action was proceeding, Beverly Watson brought another putative class-action on behalf of the roughly 2,000 individuals affected by the disappearance of the pathology reports.[61] That suit alleged the same harm as the *Beck* plaintiffs.[62] The district court also dismissed the *Watson* case for lack of subject-matter jurisdiction, holding that Watson lacked Article III standing under the Privacy Act because she failed to allege an actual or attempted misuse of the stolen information, thus her allegation that her information would be misused was speculative.[63] Both cases were consolidated on appeal by the Fourth Circuit.[64] The Fourth Circuit was asked to review whether the increased risk of identity theft that the *Beck* and *Watson* plaintiffs alleged constituted an actual or imminent injury under Article III of the Constitution.[65]

II. *BECK* SURVEYED THE CIRCUIT SPLIT AND AVOIDED PICKING A SIDE BY DRAWING FACTUAL DISTINCTIONS

This Part examines how the Fourth Circuit reached its conclusion that the occurrence of a data breach, alone, is insufficient to confer standing and that, in order to successfully plead an injury-in-fact, plaintiffs must show that thieves actually misused or attempted to misuse their stolen personal information.[66]

In February 2017, in *Beck v. McDonald*, the United States Court of Appeals for the Fourth Circuit examined whether a plaintiff could establish Article III standing by alleging that harm was impending following two da-

---

[60] *Id.* (rejecting the plaintiffs' attempt to "create standing by choosing to purchase credit monitoring services or taking any other steps designed to mitigate the speculative harm of future identity theft"). The district court also denied the *Beck* plaintiffs' request for injunctive relief under the APA, relaying on its previous analysis and holding that the injury was too speculative for the plaintiffs to assert that their information would again be compromised and that they would be injured as a result. *Id.*

[61] *Id.* at 268–69.

[62] *Id.* at 268.

[63] *Id.* at 269. The district court also dismissed the claim for injunctive relief under the APA, concluding that Watson's allegations based on Dorn VAMC's prior conduct were insufficient to show that she would be at the mercy of future data breaches and thefts in the absence of an injunction. *Id.*

[64] *Id.* at 266.

[65] *See id.* at 269.

[66] *See infra* notes 67–85 and accompanying text.

ta breaches.[67] In reviewing the consolidated appeal, the Fourth Circuit framed the issue as whether the plaintiffs met *Clapper v. Amnesty International USA*'s injury-in-fact requirement for Article III standing.[68] Specifically, the court addressed whether the plaintiffs established that the threatened injury of identity theft was certainly impending or posed a substantial risk that harm would occur under the Privacy Act.[69]

The court began its analysis by discussing the legal framework surrounding the future-injury theory of Article III standing.[70] Accordingly, the court concluded, without explanation, that *Clapper* controlled.[71] The Fourth Circuit then addressed the plaintiffs' contentions for Article III standing based on the increased risk of future identity theft and the cost of protecting against those risks.[72]

The Fourth Circuit surveyed a five-circuit split to determine whether the increased risk of future identity theft could confer standing.[73] Although acknowledging that it was possible to establish standing based on such risk, the court did not declare whether it is necessary to allege actual or attempt-

---

[67] 848 F.3d 262, 263 (4th Cir. 2017). The court had to evaluate standing at both the pleading stage and the motion to dismiss stage, but narrowed the inquiry to the motion to dismiss stage as the bar was lower and would encapsulate the summary judgment dispute. *Id.*

[68] *Id.* at 270–71; 568 U.S. 398 (2013). The court affirmed the district court's dismissals for lack of subject matter jurisdiction, agreeing with the district court's finding that the plaintiffs failed to establish injury-in-fact. *Beck*, 848 F.3d at 267.

[69] *Beck*, 848 F.3d at 270–72, 275.

[70] *Id.* at 270–72.

[71] *See id.* at 272 (discussing the appropriate standard to apply when plaintiffs allege an impending injury). The court mentioned that it would explain why it found *Clapper* to be controlling, but it does not appear like the court explicitly did. *See id.* ("*Clapper*[] . . . is controlling here. Before explaining why, we address the Plaintiffs' contention that the district court misread *Clapper* to require a new, heightened burden."). To the extent that the discussion was implicit, the court noted that the "certainly impending" standard articulated in *Clapper* was "hardly novel." *Id.* (citing DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 345 (2006); Lujan v. Defs. of Wildlife, 504 U.S. 555, 564–65 & n.2 (1992); Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). Interestingly, the court found that plaintiffs' "emotional upset" and "fear [of] identity theft and financial fraud" were insufficient to confer Article III standing—the court proceeded to limit its inquiry to a discussion of whether the increased risk of identity theft, alone, was sufficient to confer standing. *Id.*

[72] *Id.* at 273. In discussing the cost of mitigative measures, the court piggybacked on its reasoning concerning the increased risk of identity theft to deny standing. *See id.* at 276–77 (citing *Clapper*, 568 U.S. at 416) (finding the plaintiffs' arguments about the cost mitigative measures to be "a repackaged version" of their prior standing argument). The court found that, because the threat of future harm was speculative, the measures taken to mitigate that harm were "self-imposed" and could confer standing. *Id.* (citing *Clapper*, 568 U.S. at 409). For example, in support of its reasoning, the court cited *Remijas* for the proposition that mitigation costs do not satisfy the injury-in-fact requirement where the harm is not imminent. *Id.* (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015)).

[73] *See id.* at 273 (noting that the Sixth, Seventh, and Ninth Circuits have all recognized that plaintiffs can establish an injury-in-fact based on the increased risk of future identity theft and that the First and Third Circuits have rejected such contentions).

ed misuse at the motion to dismiss stage.[74] The Fourth Circuit observed that other circuits have found standing when the plaintiffs alleged that data thieves intentionally targeted personal information.[75]Those circuits relied on allegations of hacking specifically into data bases that held credit card information or misuse of that personal information soon after the breach.[76] These factors were absent in the *Beck* case.[77] Accordingly, the court found that the plaintiffs' claims were too speculative to confer Article III standing and failed to meet the certainly-impending standard.[78] The court drew similarities to *Clapper*, namely, that in order for plaintiffs to suffer the harm they fear, the court would have to participate in the same game of connect-the-dots that the Supreme Court previously rejected.[79]

---

[74] *See id.* at 273–74 (discussing the reasoning of the circuit courts but omitting to address the question).

[75] *See id.* (discussing the reasoning of the circuit courts but omitting to address the question).

[76] *See id.* at 275 (noting that threatened injuries become increasingly more speculative over time in the absence of actual misuse). For example, in support of its reasoning, the court cited *Galaria*, where the United States Court of Appeals for the Sixth Circuit in 2016 concluded that plaintiffs' increased risk of future identity theft theory established injury-in-fact after hackers targeted Nationwide Mutual Insurance Company's network and stole personal information. *Id.* at 274 (citing Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 386 (6th Cir. 2016)); *Galaria*, 663 F. App'x at 388 ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."). Similarly, in support of its reasoning, the Fourth Circuit cited *Krottner*, where the United States Court of Appeals for the Ninth Circuit in 2010 concluded, as a matter of first impression, that the plaintiffs' increased risk of future identity theft theory was sufficient to confer Article III standing following the theft of an unencrypted laptop from Starbucks that contained the personal information and social security numbers of approximately 97,000 Starbucks employees, where at least one named plaintiff was the victim of someone attempting to open an account in her name using her social security number two months after the laptop theft. *Beck*, 848 F.3d at 273–74 (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010)).

[77] *Beck*, 848 F.3d at 274. For example, the Fourth Circuit pointed out that, even after approximately four years, the *Beck* plaintiffs had produced no evidence of unauthorized access, misuse, or identity theft, nor that the thief stole the laptop with the intent to misuse their private information. *Id.* The court found that the *Watson* plaintiffs failed in the same manner. *Id.* at 274–75.

[78] *Id*. at 274-75. The court dismissed the plaintiffs' counterargument—that there was "no need to speculate" because the plaintiffs had alleged actual theft of the laptop and pathology reports—finding that the "mere theft," alone, was not grounds for Article III standing. *Id.* at 275 (citing Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007)). In support, the court cited *Randolph* for the proposition that plaintiffs must allege intent to misuse, target, or access their personal information and that a mere theft is insufficient. *Id.*

[79] *See id.* at 275 (finding that, in both cases, the thieves must first target the personal information, then select—amongst thousands of people—the personal information of the named plaintiffs and then successfully use that information maliciously). In *Clapper*, the Supreme Court denied standing because it found that the plaintiffs' alleged harm would only manifest if the Court made assumptions about the potential actions of third parties. *Clapper*, 568 U.S. at 414. For example, the Court would have had to assume that (1) the government would decide to target the specific individuals relevant to the action; (2) the government would use the specific method complained about for surveillance of those individuals; (3) the Article III judges on the Federal Intelligence Surveillance Court would authorize those surveillances; and so on. *Id.* at 410. Similarly, the Fourth Circuit, in *Beck*, found that it was too speculative to imagine what the hackers wanted with

The court also concluded that the plaintiffs failed to allege that there was a substantial risk of harm.[80] The plaintiffs claimed that 33% of data breach victims will eventually become victims of identity theft.[81] The court found, without explicit explanation, that this statistic fell short of establishing a substantial risk of harm.[82] The plaintiffs also alleged that, by offering free credit monitoring, the defendants effectively conceded the existence of a substantial risk of harm.[83] The court declined to follow its sister circuits' decisions to infer such harm from the offer, noting that such a decision would disincentivize businesses from offering those services again for fear of lawsuit. [84] Accordingly, the court found that the plaintiffs failed to show a substantial risk of harm posed by the data breaches.[85]

III. The Fourth Circuit Correctly Decided the Case, but the Legal Landscape Still Leaves Plaintiffs Uncertain How to Plead

To say the least, standing has not been applied consistently, and standing in data breach cases is no exception.[86] On one hand, it makes sense that people who target and steal personal information are likely to use it for ne-

---

the stolen laptop or stolen pathology reports, whether they knew how to access the information, or whether they would even try to access the information. *Beck*, 848 F.3d at 274.

[80] *Beck*, 848 F.3d at 275 (citing *Clapper*, 568 U.S. at 409 n.5).

[81] *Id.*

[82] *See id.* at 275–76 (finding that the statistic "falls far short" of establishing a substantial risk of harm). In support of its reasoning, the court cited *Khan* and *In re Science Applications*. *Id.* at 276 (citing Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C 2014)). Both courts found a lack of standing where plaintiffs produced statistics that showed that approximately 20% of data breach victims are sure to become the victims of identity theft. *Khan*, 188 F. Supp. 3d at 533; *In re Sci. Applications*, 45 F. Supp. 3d at 26.

[83] *Beck*, 848 F.3d at 276.

[84] *Id.* The court determined that, to use a business's altruistic offers against it would provide a disincentive for those businesses to be altruistic in the future, thus opting not to use the offer of free credit monitoring against the defendants here. *Id. But see Galaria*, 663 F. App'x at 388 ("Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year"); *Remijas*, 794 F.3d at 694 ("It is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially harmed] customers . . . . It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.").

[85] *Beck*, 848 F.3d at 276. The court, in dicta, noted that *Clapper* elucidated that a threatened event can be "reasonably likely" to occur but nonetheless fail to meet the "imminence" requirement for injury-in-fact. *Id.* (citing *Clapper*, 568 U.S. at 406–07).

[86] *See* Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc., 454 U.S. 464, 475 (1982) (discussing Article III standing generally, noting that Article III standing has not been defined consistently). *Compare* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (declining to find standing in the absence of allegations of actual misuse or harm), *with* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding standing where plaintiffs allege breach of data).

farious purposes.[87] On the other hand, as time passes and no attempts to misuse the information have occurred, it becomes harder to claim that identity theft is imminent.[88]

The Fourth Circuit in *Beck* correctly arrived at this conclusion.[89] The unfortunate reality, however, is that data breach victims are now left asking how and when should they bring a lawsuit: what facts must be pleaded for their case to proceed; and should they wait until they have evidence of hackers trying to use their stolen information, or sue as soon as they hear that a breach has occurred?[90] This Part argues that victims are left asking themselves those questions with no answer in sight.[91] Specifically, this Part argues that the Fourth Circuit properly determined that the plaintiffs lacked standing and also identifies that, where data breaches occur from physical theft, like that of a laptop, plaintiffs seem to struggle the most to establish standing.[92]

The Fourth Circuit correctly determined that the *Beck* and *Watson* plaintiffs failed to allege facts to make it plausible that their injuries were imminent.[93] While evaluating whether identity theft was certainly impend-

---

[87] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (commenting on the imminence of future identity theft as seeming to be the purpose for stealing information); WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 20 (noting the inconsistencies amongst courts where plaintiffs allege increased risk of identity theft without actual or attempted misuse).

[88] *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 958–60 (D. Nev. 2015) (finding that the plaintiffs lacked standing where years had passed without the plaintiffs making any allegations of misuse); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366–67 (M.D. Pa. 2015) (noting that a lapse of time undermines the concept of "imminent").

[89] *See* Beck *v.* McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (discussing that plaintiffs have failed to show any indication their stolen personal information would be used in a way that would cause them harm just because a laptop and pathology reports were stolen).

[90] *See Remijas*, 794 F.3d at 694 (noting the inherent difficulty in requiring data breach plaintiffs to wait for harm to manifest before bringing a lawsuit); *see also* WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 20 (noting the difficult choices data breach victims have to make when deciding whether to bring a lawsuit and what to plead); Dowty, *supra* note 3, at 686–87 (noting a circuit split concerning the sufficiency of allegations required to confer standing); Lee & Ellis, *supra* note 28, at 180 (discussing the complexity of the relationship between proving an impending injury and proving that your case has been properly incubated such that it is "ripe" for trial).

[91] *See infra* notes 93–110 and accompanying text.

[92] *See infra* notes 93–110 and accompanying text.

[93] *Beck*, 848 F.3d at 267 (denying plaintiffs standing where they suffered no economic harm as a result of having their personal information stolen by a laptop thief). This argument is made on the assumption that *Clapper* was correctly decided and applies in data breach class actions. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (permitting a substantial risk theory). *See generally* Green, *supra* note 30 (discussing the possibility that the substantial risk test is a fiction created to secure Justice Kennedy's vote). One might argue that *Clapper*'s effect does not quite reach private collection of private information, as *Clapper* was a case about a *public* collection of private information by the government through FISA. *See, e.g.*, 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, 15, 50 (2014), https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1405&context=jolt [http://perma.cc/9H8B-KSWW] (discussing the ensuing split between courts in the data breach sphere before and after *Clapper*, assuming,

ing, the court compared the plaintiffs' allegations to cases where increased risks of identity theft were sufficient to confer standing.[94] Accordingly, the court identified three failures within the plaintiffs' case: (1) a lack of intent by the thieves to target the personal information of the victims; (2) a lack of attempt at misuse; and (3) a lack of actual misuse.[95] Virtually no courts have granted standing in the absence of all three of the above allegations, and all three were missing in this case.[96] Irrespective of whether allegations of actual misuse are required to confer standing, no court has been willing to label an identity theft "imminent" unless a thief, at the very least, targeted or attempted to misuse personal information within a reasonable amount of

---

without explanation, that *Clapper* properly applies in data breach cases). Courts are even torn as to the effect of *Clapper* in data breach cases. *Compare In re Zappos*, 108 F. Supp. 3d at 956 (citing *In re* Sony Gaming Networks & Consumer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014)) (discussing Article III standing requirement, noting that, although *Clapper* did not use the Ninth Circuit's "real and immediate" language, it "did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate'"), *with* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 (N.D. Ill. 2014) (discussing *Clapper*'s effect on future injury-in-fact, noting "*Clapper* expressly rejected the . . . 'objectively reasonable likelihood standard' as 'inconsistent with our requirement that threatened injury must be certainly impending to constitute injury-in-fact'"). Obviously, if it turns out that *Clapper* precludes increased risk theories for future identity theft, then the holding that the plaintiffs' allegations of harm were too speculative was accurate. *See Beck*, 848 F.3d at 274 (finding that the plaintiffs did not adequately plead an increased risk of identity theft). *Compare* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (acknowledging the viability of a substantial risk theory of injury in fact), *with* Blum v. Holder, 744 F.3d 790, 797 (1st Cir. 2014) (applying *Clapper*'s certainly impending standard, discussing the ambiguity in *Clapper*). Likewise, if *Clapper* is to be understood as allowing increased risk of injury theories to confer standing in the data breach context, then the Fourth Circuit was also correct to undertake the analysis and affirm the decision to dismiss the case. *See Beck*, 848 F.3d at 274 (finding that plaintiffs failed to allege they were at an increased risk of identity theft following a data breach). *Compare Spokeo*, 136 S. Ct. at 1549 (acknowledging the viability of a substantial risk theory of injury in fact), *with Blum*, 744 F.3d at 797 (applying *Clapper*'s certainly impending standard, discussing the ambiguity in *Clapper*).

[94] *Beck*, 848 F.3d at 274.

[95] *Id.* (discussing the facts and rationale sister circuits employed when finding standing, noting that "plaintiffs ma[d]e no such [similar] claims"); WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 19 (listing a compilation of factors by which courts have found standing, and noting factors where the absences have been fatal to plaintiffs' cases).

[96] *See* WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 18 (noting that, to even have a chance at a court finding standing, plaintiffs need to allege a minimum of data breach coupled with a statutory violation); Dowty, *supra* note 3, at 689–93 (surveying the circuit split and discussing the factors courts have discerned confer standing). Assuming that the pathology reports were stolen and not merely misplaced, one can argue that the thieves in *Beck* "targeted" the pathology reports for the social security numbers and medical history contained therein. *See Beck*, 848 F.3d at 268. Targeting the information notwithstanding, the passage of four years without a single incidence of attempted misuse severely dampens a claim that future identity theft is imminent. *See In re Zappos*, 108 F. Supp. 3d at 958–60 (finding that the plaintiffs lacked standing where years had passed without the plaintiffs making any allegations of misuse); *Storm*, 90 F. Supp. 3d at 366–67 (noting that a lapse of time undermines the concept of "imminent").

time following the breach.[97] If there hasn't been at least one unauthorized attempt at a person's identity over four years since the data exposure, it is indefensible to claim that identity theft is *still* certainly impending.[98] Moreover, the plaintiffs had not alleged that their medical insurance, credit cards, bank accounts, or other personal accounts had been subject to attempts at unauthorized access.[99]

The Fourth Circuit was also correct that the plaintiffs' argument concerning the "substantial risk" of harm posed by the compromised laptop and

---

[97] *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (finding standing where a thief stole a laptop containing unencrypted personal information of over 97,000 Starbucks employees, where at least one plaintiff alleged misuse in the form of a fraudulent attempt to open a bank account); *Attias*, 865 F.3d at 623, 629 (finding standing where a thief stole two laptops and subsequent misuse was alleged). Indeed, scholars have insinuated that the mere theft of information, by itself, poses no harm to the owner of the information without subsequent use; the use of personal information is what deprives the original owner of the information's value, thus making it fair to say the victim had been harmed. *See* STUART P. GREEN, 13 WAYS TO STEAL A BICYCLE: THEFT LAW IN THE INFORMATION AGE 244 (2012) (proposing that unless one's stolen personal information is misused, it is hard to claim that the victim had been harmed). One scholar drew a useful analogy to the Takings Clause of the Fifth Amendment: in instances of governmental takings, plaintiffs are compensated only when the takings "go too far." *Id.* Similarly, identity theft won't confer an injury unless the thief has gone "too far" and took steps towards depriving someone of property value. *Id.* For an example of when the government went "too far," consider *Pennsylvania Coal Co. v. Mahon*, where the plaintiffs sought an injunction to prevent a coal company from mining below their home to prevent the ground from collapsing beneath their feet. 260 U.S. 393, 414–15 (1922). There, the issue was whether the coal company could be prevented from digging out the valuable coal support pillars that kept the ground from collapsing, or whether the preventative statute would amount to an impermissible regulatory taking by the government. *Id.* The court, finding for the coal company, decided that a statute that prevented the coal company from mining the remaining foundational coal would deprive the company of the subterranean property value, thus going "too far" and requiring compensation to the company for the loss as if it were a taking. *Id.* In *Beck*, the Fourth Circuit's decision makes sense in light of this analogy: accepting the plaintiffs' allegations as true, although thieves stole pathology reports containing, *inter alia*, names and social security numbers, there is something to be said for nearly four years passing without an instance of attempted misuse or actual misuse. *See Beck*, 848 F.3d at 275 (noting a connection between the passing of time and the speculative nature of an allegedly impending harm); *see also In re Zappos*, 108 F. Supp. 3d at 958 (noting that the passage of time is a factor to weigh when considering how "impending" an alleged injury is, and that the more time passes, the more plaintiffs' arguments are "undermined"). Because there was no harm, or an action that looks like an attempt to cause harm, plaintiffs should not be compensated. *See Beck*, 848 F.3d at 274 (denying standing where the plaintiffs failed to allege that there had been any attempts by thieves to misuse their stolen information).

[98] *See Beck*, 848 F.3d at 275 (noting that plaintiffs "uncovered no evidence that the information contained on the stolen laptop has been accessed or misused"); *In re Zappos*, 108 F. Supp. 3d at 958–60 (finding that the plaintiffs lacked standing where years had passed without the plaintiffs making any allegations of misuse); *Storm*, 90 F. Supp. 3d at 366–67 (noting that a lapse of time undermines the concept of "imminent").

[99] *Beck*, 848 F.3d at 274. The court pointed out that the *Beck* plaintiffs *could not* have been the victims of credit or bank fraud because the stolen laptop did not contain any credit card or bank account information. *Id.* at 274 n.6. *But see Attias*, 865 F.3d at 628 (finding that the theft of merely a combination of names, birthdays, email addresses, and subscriber identification numbers could confer standing because the risk of medical insurance fraud was sufficiently high).

pathology reports carried little weight.[100] The plaintiffs offered generalized statistics concerning identity theft following data breaches in the abstract.[101] As the court noted, these statistics provided no insight into the particular facts of the case.[102] Absent particular assessments of the risks posed to these plaintiffs under the *type* of theft, it cannot be said that *these* victims face a "substantial risk" of harm.[103] Moreover, the court properly chose not to interpret Dorn VAMC's offer to monitor the victims' credit scores as proof of a "substantial risk."[104] As the court noted, it would be poor policy to slap an altruistic wrist as it might deter future benevolent attempts to mitigate potential harm.[105]

---

[100] *See Beck*, 848 F.3d at 275–76 (denying plaintiffs standing where they failed to allege that identity theft would follow from the theft of a laptop and pathology reports); *Clapper*, 568 U.S. at 410 (noting that "allegations of possible future injury are not sufficient" to confer standing (internal citations omitted)). Increased risk of identity theft, alone, may be sufficient to confer standing in certain circumstances. *See Attias*, 865 F.3d at 629 (finding that plaintiffs adequately pleaded injury-in-fact based on an increased risk of identity theft theory). For example, in *Attias*, an unknown hacker breached twenty-two computers and accessed a database that contained customers' credit card numbers and full social security numbers (as opposed to only the last four digits). *Id.* at 623. The court, finding standing, reasoned that when a company collects personal information in the form of credit card and social security numbers, and that information is targeted and accessed, plaintiffs are at a high risk of financial fraud. *Id.* at 629. Of course, the court would have to make assumptions that the hacker who took that information would then use it for nefarious purposes. *See, e.g.*, *Remijas*, 794 F.3d at 693 ("Why else would hackers break into a store's database and steal customers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities."). Nevertheless, that assumption is much more sensible when the facts reveal that a hacker aimed their hack at that personal information, rather than, for example, stole a laptop. *Compare Beck*, 848 F.3d at 275 (noting that the mere theft of an item, alone, is insufficient to confer Article III standing, requiring that plaintiffs show allegations of attempted or actual misuse of the stolen personal information), *with Remijas*, 794 F.3d at 693 (finding standing where hackers deliberately aimed their attack at personal credit card information and fraudulent credit card charges appeared on customers' credit card statements soon thereafter).

[101] *Beck*, 848 F.3d at 275–76.

[102] *See id.* at 275 n.7 (noting that plaintiffs' "general statistic [said] nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case").

[103] *Id.*; *see* Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) (noting that statistics, which are often cited in other cases of a similar sort, do not establish that identity theft is "certainly impending" in the instant case). It is simply too conjectural to apply generalized statistics to the facts of a case. *Khan*, 188 F. Supp. 3d at 533.

[104] *Beck*, 848 F.3d at 276. *But see* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year."); *Remijas*, 794 F.3d at 694 ("It is telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all [potentially harmed] customers . . . . It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."). Offering free credit monitoring following a data breach is not an uncommon occurrence. *See* Regnier & Woolley, *supra* note 1 (noting that Equifax offered free credit-monitoring services following a breach).

[105] *Beck*, 848 F.3d at 276; *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 634 & n.12 (3d Cir. 2017) (commenting that an offer by a company to monitor credit follow-

The fallout from the *Beck* decision and the current circuit split is disconcerting: victims either have to wait for harm to materialize or allege—at the very least—that thieves specifically targeted their personal information to even have a shot at establishing standing.[106] In instances of laptop thefts, it is difficult to imagine these cases proceeding past the standing phase on increased-risk theories without some allegations of actual harm or attempted misuse, forcing victims to wait before they can bring a lawsuit.[107] The issue is particularly salient in laptop theft cases because the mere theft of a laptop does not necessitate that the thief wanted the information contained within.[108] Even if victims can allege that the laptop was targeted for personal information, courts are inconsistent as to whether the mere *targeting* of personal information is sufficient to confer standing.[109] This, in turn, will force victims to sit and wait for at least an *attempt* by a thief to access their personal information before filing a suit.[110]

CONCLUSION

In February 2017, in *Beck v. McDonald*, the Fourth Circuit held that allegations that a laptop and pathology reports were stolen did not mean that identity theft was imminent. The court further held that, even though personal information was contained within the stolen items, there was no evidence that the thief intended to use that personal information for nefarious purposes. This decision deepened a circuit split surrounding what allegations are sufficient to show that identity theft is imminent following a data breach. Victims are now stuck between a rock and a hard place: they live in fear that their identities may be compromised at any minute, yet lack the standing to obviate their anxieties through judicial remedy. In a society that is ever-increasingly

---

ing a breach should not be seen as a "concession or recognition" that plaintiffs suffered an injury, or else companies may be disincentivized in future instances).

[106] *See Remijas*, 794 F.3d at 693 (noting the traceability problem created by plaintiffs having to wait for harm to materialize before bringing a lawsuit); WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 20 (same).

[107] *See, e.g.*, *Attias*, 865 F.3d at 629 (finding standing following the theft of two laptops where subsequent misuse was alleged); Resnick v. AvMed, Inc., 693 F.3d 1317, 1321–22 (11th Cir. 2012) (finding plaintiffs met the requirements of Article III standing where two unencrypted laptops were stolen and sold to someone who had a history of dealing in stolen property, and where actual identity theft and misuse were alleged); *Krottner*, 628 F.3d at 1142 (noting that a named plaintiff had someone try to open up a bank account in his name following the laptop theft).

[108] *See Beck*, 848 F.3d at 274 (noting that the plaintiffs failed to allege that the laptop thief deliberately targeted their personal information).

[109] Beatty, *supra* note 1, at 1290 (discussing that, in order to find standing, courts require that plaintiffs show more than merely that their data had been stolen, and must bring forth allegations and evidence of misuse, and economic damages).

[110] *See Remijas*, 794 F.3d at 693 (noting the traceability problem created by plaintiffs having to wait for harm to materialize before bringing a lawsuit); WHAT'S "NEW" IN CYBERSECURITY, *supra* note 2, at 20 (same).

dependent on trusting businesses with our personal information, instances of data breach litigation are only bound to rise. Until the Supreme Court clarifies the requirements for injury-in-fact within the data breach context, plaintiffs will be continuously rolling the dice on whether they actually are harmed before they ever approach the merits of their claims.

BRANDON FERRICK

Preferred Cite: Brandon Ferrick, Comment, *No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions*, 59 B.C. L. REV. E. SUPP. 462 (2018), http://lawdigitalcommons.bc.edu/bclr/vol59/iss6/462.