Washington and Lee Law Review Online

Volume 73 | Issue 1 Article 3

6-1-2016

Clapper Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison

Arthur R. Vorbrodt
Washington and Lee University School of Law

Clapper Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison

Arthur R. Vorbrodt*

Table of Contents

* Candidate for J.D., Washington and Lee University School of Law, May 2017. I would like to thank Professor Doug Rendleman for serving as my Note advisor and Elaine McCafferty for serving as my Note editor.

I. Introduction

"It's a bad week to have been conducting an extra-marital affair."[1] The Ashley Madison data breach on August 18, 2015, achieved nationwide notoriety[2] and is just one of many examples of large-scale data breach that have occurred within the last few years.[3] AshleyMadison.com is an adult dating website that matches married men and women looking for "casual encounters, married dating, discreet encounters, and extramarital dating"; its slogan is, "Life is short. Have an affair."[4] A group of hackers

---

1. *See* Zahra Mulroy, *Ashley Madison Hack: Cheaters and Victims' Reactions Are NOT What You Expect*, MIRROR (July 22, 2015), http://www.mirror.co.uk/lifestyle/sex-relationships/ashley-madison-hack-cheaters-victims-6112966 (last visited May 12, 2016) (predicting the likely repercussions of the Ashley Madison data breach and subsequent dissemination of customer information) (on file with the Washington and Lee Law Review).

2. *See* Adrienne LaFrance, *What Everybody Googled in 2015*, ATLANTIC (Dec. 16, 2015), http://www.theatlantic.com/technology/archive/2015/12/what-everybody-googled-in-2015/420717/ (last visited May 12, 2016) (reporting "What is Ashley Madison" as a top 10 Google search in 2015) (on file with the Washington and Lee Law Review).

3. *See* Grave Gavilanes, *Hackers Access Ashley Madison Site, Data Expose Online Cheaters*, PEOPLE (July 20, 2015, 4:00 PM), http://www.people.com/article/ashley-madison-site-hack (last visited May 12, 2016) (discussing the release of a statement by Avid Life Media, Inc.—owner of AshleyMadison.com—confirming unauthorized access by hackers to confidential customer information) (on file with the Washington and Lee Law Review). For just a few instances of data breaches occurring in October 2015 alone, see Eric Chabrow, *Scottrade Belatedly Learns of Breach*, DATA BREACH TODAY (Oct. 2, 2015), http://www.databreachtoday.com/scottrade-belatedly-learns-breach-a-8565 (last visited May 12, 2016) (noting that law enforcement notified Scottrade—a discount brokerage—of a cyber attack in late September 2015) (on file with the Washington and Lee Law Review); Mathew J. Schwartz, *Experian Faces Congressional Scrutiny over Breach*, DATA BREACH TODAY (Oct. 9, 2015), http://www.databreachtoday.com/experian-breach-congress-investigates-a-8580 (last visited May 12, 2016) (discussing a recent data breach of Experian—an online securities trading company) (on file with the Washington and Lee Law Review); Karl Thomas, *Dow Jones & Company Experiences Data Breach*, WELIVESECURITY (Oct. 12, 2015, 2:31 PM), http://www.welivesecurity.com/2015/10/12/dow-jones-company-experiences-data-breach/ (last visited May 12, 2016) (examining the October 12, 2015 data breach of Dow Jones) (on file with the Washington and Lee Law Review).

4. ASHLEY MADISON, https://www.ashleymadison.com (last visited May 12, 2016) (on file with the Washington and Lee Law Review).

known as "Impact Team" stole the confidential records and information of over 37 million Ashley Madison users.[5] After a series of threats demanding that Avid Life Media, Inc.—AshleyMadison.com's owner—shut down the website, Impact Team publicly released the records.[6]

Data breaches are a part of life in the modern technological world.[7] Compilation of customer data is the norm for large corporations and small businesses alike.[8] As a result, online hackers have developed sophisticated hacking methods capable of circumventing complex security systems and acquiring the sensitive customer information on their data servers.[9] Once stolen, this data—known as personally identifiable information (PII)—greatly increases the victim's likelihood of identity theft.[10] PII can be any information from customer phone numbers and home addresses to credit card information, medical information, and social security numbers.[11] Identity thieves use this highly

---

5. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (last visited May 12, 2016) (detailing the public release of the hacked user information) (on file with the Washington and Lee Law Review).

6. *See id.* ("The hackers deflected responsibility for any damages or repercussions that victims of the breach and data dump may suffer. 'Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages . . . .'").

7. *See infra* note 14 and accompanying text (providing a representative list of recent large-scale data breaches).

8. *See* Robert Faturechi, *FTC Calls for Curbs on Consumer Data Collection*, L.A. TIMES (May 27, 2014), http://www.latimes.com/business/la-fi-ftc-data-brokers-20140528-story.html (last visited May 12, 2016) ("The FTC found that data brokers collect and store billions of data points covering nearly all American consumers.") (on file with the Washington and Lee Law Review).

9. *See* Matt Johansen, *Top 10 Web Hacking Techniques of 2014*, WHITEHAT SEC. (Mar. 19, 2015), https://blog.whitehatsec.com/top-10-web-hacking-techniques-of-2014/ (last visited May 12, 2016) (listing over thirty different data theft techniques used in 2014 alone) (on file with the Washington and Lee Law Review).

10. *See* Tim Chen, *Identity Theft: Your Chances of Being a Victim*, U.S. NEWS (Mar. 23, 2011), http://money.usnews.com/money/blogs/my-money/2011/03/23/identity-theft-your-chances-of-being-a-victim (last visited May 12, 2016) (noting that, in 2011 alone, 250,854 Americans were victims of identity theft) (on file with the Washington and Lee Law Review).

11. *See* ARVIND NARAYANAN & VITALY SHMATIKOVV, MYTHS AND FALLACIES OF "PERSONALLY IDENTIFIABLE INFORMATION" 1 (2010) (determining PII includes Social Security numbers, driver's license numbers, and financial accounts).

personal data—particularly social security numbers—to open false credit cards, gain access to private bank accounts, etc.; others make a profit selling the PII on the Internet.[12]

Dozens of large companies—and even the federal government—became data breach victims over the past decade.[13] The most notable commercial data breaches targeted CareFirst BlueCross BlueShield, J.P. Morgan, Yahoo, Neiman Marcus, Target, Sony PlayStation and Online Entertainment Networks, Citigroup, MasterCard, Visa, and Starbucks.[14] The Ashley Madison data breach in particular serves to remind the public and the legal community of data breaches' harsh consequences.[15]

---

12. *See* Michael Riley, *Stolen Credit Cards Go for $3.50 at Amazon-Like Online Bazaar*, BLOOMBERG (Dec. 20, 2011, 12:01 AM), http://www.bloomberg.com/news/articles/2011-12-20/stolen-credit-cards-go-for-3-50-each-at-online-bazaar-that-mimics-amazon (last visited May 12, 2016) (reporting that identity thieves steal 8.4 million credit card numbers on average annually, many of which can be sold at around $3.50 per card) (on file with the Washington and Lee Law Review). The information normally includes the cardholder's name, address, and credit card security code. *Id.*

13. *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ (last visited May 12, 2016) (examining the cyber attack against the federal government where the personal information of 22 million government employees was compromised) (on file with the Washington and Lee Law Review).

14. *See Data Breach Lawsuits and Information*, MORGAN & MORGAN, http://www.forthepeople.com/class-action-lawyers/data-breaches/ (last visited May 12, 2016) (providing a list of notable data breaches within the past ten years) (on file with the Washington and Lee Law Review). Other large-scale data breaches targeted Premera Blue Cross, UPS Stores, Inc., Lowe's, eBay, Kaiser Permanente, Sears Holdings Corp., New York State Electric & Gas Co., Valve/Steam, Lincoln Financial Group, Gap, Staples, and Hewlett Packard. *Id.*

15. *See* Robin Levinson King, *Ashley Madison Customers Complain of Blackmail After Hack*, TORONTO STAR (Nov. 18, 2015), http://www.thestar.com/news/privacy-blog/2015/11/ashley-madison-customers-complain-of-blackmail-after-hack.html (last visited May 12, 2016) (discussing the blackmailing of several Ashley Madison customers following the breach) (on file with the Washington and Lee Law Review); Sara Malm, *Two Suicides Are Linked to Ashley Madison Leak: Texas Police Chief Takes His Own Life Just Days After His Email Is Leaked in Cheating Website Hack*, DAILY MAIL (Aug. 24, 2015), http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html (last visited May 12, 2016) (reporting on two suicides allegedly connected to the Ashley Madison data breach) (on file with Washington and Lee Law Review); Zetter, *supra* note 5 (finding that the stolen information contained names, email addresses, home addresses, amounts paid and the last four digits

The issue of Article III standing[16] for data breach lawsuits is especially relevant in the Ashley Madison data breach.[17] A plaintiff must suffer an invasion of a legally protected interest to establish standing; this invasion must be "concrete and particularized" and "actual or imminent."[18] This presents a serious issue for victims of data breach; an unknown party wrongfully accessed their data, thereby increasing their risk of identity theft, but causing no actual injury to confer standing to sue.[19] Furthermore, courts' interpretations of what constitutes an imminent injury are divided, to say the least.[20] This presents a scenario where the parties have not suffered an "actual injury,"[21] and, under some courts' rulings, their increased risk of harm does not rise to the "imminent" level.[22] Yet, they will likely be seeking a remedy from the service provider for injuries that have not yet occurred.[23]

---

of customer credit cards).

16. *See* U.S. CONST. art. III, § 2 (granting federal courts jurisdiction over "cases and controversies . . . between citizens of different states"); *infra* Part II (discussing the tripartite Article III standing requirements of injury in fact, causation, and redressability).

17. *See infra* Part II.B (discussing the relative ease of establishing standing once leaked information is used against the consumer—as compared to where the customer has yet to be "injured").

18. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992) (establishing fundamental article III standing requirements).

19. *See infra* Parts III–VI (arguing that a targeted breach increases a victim's risk of identity theft to a level that any future harm can be considered imminent).

20. *See infra* notes 24–25 (comparing the vastly different outcomes for similar cases at the district and circuit court levels).

21. *See Lujan*, 504 U.S. at 561 (establishing the "actual injury" requirement as "indispensible" to a plaintiff's case).

22. *See* cases cited *infra* notes 24–25 (listing data breach class action cases, many of which the courts rule against plaintiffs who were not yet victims of identity theft).

23. *See* David S. Almeida & Mark Eisen, *Barbarians at the Gate: Seventh Circuit Finds Article III Standing for Data Breach Class Actions*, LEXOLOGY: CLASS ACTION DEF. STRATEGY BLOG (July 24, 2015), http://www.lexology.com/library/detail.aspx?g=4fd79797-228b-4930-9351-11f3145cb1ef (last visited May 12, 2016) (finding that "[t]he overwhelming majority of courts . . . dismiss data breach actions for the simple reason that until a consumer suffers *actual* identity theft, she lacks Article III standing to sue") (on file with the Washington and Lee Law Review).

Outcomes are mixed at the federal district court level,[24] but the few circuits to address the issue have traditionally been

24. *Compare* Maglio v. Advocate Health & Hosps. Corp., 2015 IL App (2d) 140782-U, at *6 (Ill. App. Ct. June 2, 2015) (dismissing an action where burglars stole company computers with customer information for failure to show actual harm because "[t]he increased risk that plaintiffs will be identity theft victims at some indeterminate point in the future . . . . [D]id not constitute an injury sufficient to confer standing"), *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("[I]ncreased risk of harm alone does not constitute an injury in fact. Nor do measures taken to prevent a future, speculative harm."), Allison v. Aetna, Inc., No. CIV.A. 09-2560, 2010 WL 3719243, at *6 (E.D. Pa. Mar. 9, 2010) (holding that the plaintiff lacked standing where an online phishing scam compromised plaintiff's PII, but the plaintiff had not yet suffered concrete harm), Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1051–53 (E.D. Mo. 2009) (ruling that the risk of future harm posed by future data theft where the harm may not occur is too speculative), Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (same), Polanco v. Omnicell, Inc., No. 13–1417, 2013 WL 6823265, at *14 (D.N.J. Dec. 26, 2013) (relying on *Clapper v. Amnesty Int'l USA* and *Reilly v. Ceridian Corp.* to conclude that mere loss of data, without misuse, is not "an injury sufficient to confer standing"), Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("*Clapper* compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."), Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d. 646, 660 (S.D. Ohio 2014) (holding that the increased risk of future harm relying on the occurrence of future criminal actions by independent decision-makers was not imminent), *and In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Cal. Mar. 3, 2013) ("The Complaint alleges Plaintiffs incurred expenses to mitigate an increased risk of identity theft or fraud, but it does not allege what those expenses are with any specificity. *Even if specific expenses had been alleged*, such expenses would not qualify as actual injuries under *Clapper*." (emphasis added)), *with In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d. 1197, 1212 (N.D. Cal. 2014) (limiting *Clapper* to its facts and granting standing on the grounds that the data breach placed plaintiffs in immediate danger), Enslin v. Coca-Cola Co., No. 2:14-CV-06476, 2015 WL 5729241, at *5 (E.D. Pa. Sept. 30, 2015) (finding standing where plaintiff's bank account had been fraudulently accessed—representing an actual injury), *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding plaintiffs to have standing where their credit cards were used to make unauthorized purchases), *In re* Zappos.com, Inc., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (finding standing where the plaintiffs suffered "actual fraud or identity theft"), Holmes v. Countrywide Fin. Corp., No. 5:08–CV–00205–R, 2012 WL 2873892, at *5 (W.D. Ky. July 12, 2012) (finding that the plaintiffs suffered an injury-in-fact because they were required to expend time and money to protect their identity), *and* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014) (distinguishing *Clapper,* "conclud[ing] that the elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing"). "This conclusion follows from *Pisciotta* and is consistent with a host of Supreme Court decisions finding standing based on an imminent

favorable to plaintiffs.[25] More recently, however, district courts interpret *Clapper v. Amnesty International USA*[26]—a non-data breach Supreme Court case published in 2013—to foreclose the use of imminent injury in data breach lawsuits, trumping the plaintiff-friendly circuit opinions.[27] The majority of post-*Clapper* district court cases applied *Clapper*—incorrectly—to dismiss imminent injury claims for lack of standing.[28] These courts focused on the "injury" prong, reasoning that, if a plaintiff's future injury relies on speculation, then it is not certainly impending and, therefore, it fails the imminent injury requirement.[29]

The U.S. Court of Appeals for the Seventh Circuit in *Remijas v. Neiman Marcus Group, LLC*,[30] however, broke this district court trend and found standing in a data breach action despite the Supreme Court's *Clapper* decision, finding that *Clapper* did

---

risk of future injury." *Moyer*, 2014 WL 3511500, at *6.

25. *Compare* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (concluding that "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 harm* that the plaintiff would have otherwise faced, absent the defendants actions" (emphasis added)), *and* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding that faced "a credible threat of harm" that was "both real and immediate, not conjectural or hypothetical" (internal citations omitted)), *with* Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008) (denying standing for plaintiff's claims of harm from future identity theft on the grounds that they were hypothetical and conjectural), *and* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (finding no injury-in-fact where the plaintiff"s PII was accessed but not yet misused).

26. 133 S. Ct. 1138 (2013).

27. *See id.* at 1147 (denying standing for plaintiffs on the grounds that, because a speculative chain of events had to occur for the plaintiffs to be injured, the injury was not imminent). *Clapper* is the seminal case courts use to address whether an "uninjured" plaintiff suing for damages has standing resulting—many courts have followed the *Clapper* Court's reasoning in denying standing. *See infra* Part III.A.3 (discussing cases denying standing in light of *Clapper* even though *Clapper* was not a data breach case).

28. *See infra* Part III.C (critiquing a few notable district court interpretations of *Clapper*).

29. *See Galaria*, 998 F. Supp. 2d. at 654–55 (interpreting *Clapper* as a barrier for data breach plaintiffs who have yet to suffer an actual injury (citing *Clapper*, 133 S. Ct. at 1143)). Speculation is inherent in any imminence theory and courts have incorrectly interpreted *Clapper* to disallow any speculation and heighten standing requirements altogether. *See infra* Part V.A.2 (arguing that even the certainly impending standard allows a degree of speculation).

30. 794 F.3d 688 (7th Cir. 2015).

not change the law on standing.[31] In light of this recent circuit split, this Note examines whether plaintiffs in data breach lawsuits can raise the Seventh Circuit's decision in *Remijas* to argue standing even without suffering an actual injury.[32] Specifically, it asks whether standing for data breach lawsuits can survive on imminent injury alone after *Clapper*.[33]

Part II of this Note provides a brief history and discussion of standing.[34] This discussion establishes the fundamental elements of standing a plaintiff must satisfy for her claim to be heard in court.[35] It focuses on the injury-in-fact prong, but the issue warrants a brief discussion of the causation and redressability elements as well.[36] Part II further discusses the standing issues that data breach plaintiffs face;[37] it describes how courts consider claims of actual harms, future harms, and mitigation costs in determining standing.[38] Part III provides a selective discussion of the current state of data breach standing case law.[39] This

---

31. *See id.* at 693 (holding that plaintiffs in a data breach involving Neiman Marcus "should not have to wait until hackers commit identity theft or credit-card fraud to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur" (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1338, 1147 (2013)). For an article discussing the Seventh Circuit's denial of an en banc review for *Remijas*, see Mao Shiokura, *7th Cir: Neiman Marcus Data Breach Injuries Sufficient for Article III Standing*, IMPACT LITIG. J. (Sept. 23, 2015), http://www.impactlitigation.com/2015/09/23/7th-cir-neiman-marcus-data-breach-injuries-sufficient-for-article-iii-standing/ (last visited May 12, 2016) (on file with the Washington and Lee Law Review).

32. *See infra* Part V (positing that *Remijas* properly limits *Clapper* to its facts, rendering it inapplicable in data breach context).

33. *See infra* Part V (defending the *Remijas* and *Adobe* courts' interpretation of *Clapper*).

34. *See infra* Part II (setting forth requirements for Article III standing and discussing their respective relevance with regard to data breach).

35. *See infra* Part II (discussing the actual or imminent injury, traceability, and causation requirements of Article III standing).

36. *See infra* Part II (noting that, even if a plaintiff establishes an injury, the injury must be "fairly traceable" to the defendants actions and a favorable court ruling must be capable of providing a remedy for the alleged harms).

37. *See infra* Part III (requiring data breach victims, who yet to have their information misused, to establish that any future harms are so imminent as to prove an almost inevitable likelihood of them occurring).

38. *See infra* Part III (discussing the difficulties facing data breach plaintiffs who have yet to suffer actual harms—such as fraudulent credit card transactions).

39. *See infra* Part IV (analyzing the material factual distinctions between

discussion includes pre-*Clapper* circuit court cases ruling for and against standing. Pre-*Clapper* case law is particularly relevant because, this Note argues, *Clapper* did not change the law and the pre-*Clapper* standards still apply.[40] Part III also discusses *Clapper* as well as the cases that interpret it to foreclose future injury claims in data breach cases.[41] At the same time, Part III introduces the cases that correctly apply *Clapper* and take it for what it is; a non-data breach case with minimal to no effects on standing law.[42] Most importantly, Part IV introduces *Remijas*—the first post-*Clapper* circuit court to consider imminent injury in data breach lawsuits.[43]

Finally, Part V argues that *Clapper* should be limited to its facts and applied only to cases where a chain of events is truly speculative and, therefore, not sufficiently imminent.[44] But, *Clapper* does not apply where a data-breach directly jeopardizes personal customer information and no additional steps are required for identity thieves to use the data against the victims.[45] Part V argues that the increased risk of identity theft is not "possible"[46] when hackers have direct access to the personal information; rather, it is "imminent."[47] Identity theft is sufficiently imminent to be considered "certainly impending"

---

cases in which standing was granted and when standing was denied).

40. *See infra* Part III.A (discussing pre-*Clapper* circuit court precedent).

41. *See infra* Parts III.B–C (analyzing *Clapper* and discussing the lower courts' reasoning for applying it broadly).

42. *See infra* Part III.D (citing cases that limit *Clapper* to its facts).

43. *See infra* Part IV (setting forth and distinguishing federal and circuit courts' reasoning for granting standing in light of *Clapper*).

44. *See infra* Part V (arguing that, while *Clapper*'s holding was proper in light of the facts, the Supreme Court did not intend to tighten the current standard for standing).

45. The *Remijas* court employed similar reasoning. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 696 (7th Cir. 2015) (finding that, once data thieves obtained unencrypted customer data, the breach created a "substantial risk" of future identity theft).

46. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154 (2013) (denying standing where plaintiffs argument relied merely on *possible* government actions unknown to the plaintiffs).

47. *See* Whitmore v. Arkansas, 495 U.S. 149, 156–60 (1990) (establishing the requirement that an injury must be "certainly impending" to create an imminent injury sufficient to confer standing).

when hackers have unfettered access to data.[48] This Note argues that once PII is stolen and readily accessible, there is a cognizable imminent injury. At that point, identity theft is no longer a question of "if," but rather, a question of "when."

II. Constitutional Standing

A. Fundamental Principles

"No principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases and controversies."[49] Standing is based on the fundamental principle of separation of powers and is designed to prevent the judicial branch from usurping the powers of other political branches.[50] In the context of government action, if a court were to accept any case on mere speculation or generalized grievances, it would be unrightfully asserting its decisionmaking power in a field specifically reserved to the Legislative or Executive Branches.[51]

---

48. *See Clapper*, 133 S. Ct. at 1141 (finding that plaintiffs' injuries were too speculative to be considered imminent because a series of five events needed to occur before plaintiffs were actually injured).

49. *See* DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (denying standing for plaintiff taxpayers alleging a decrease in city tax funds where an automobile manufacturer was given a tax credit, and thus, sustaining an injury city residents). This case exemplifies the importance of standing acting as a filter, protecting the courts and government entities from generalized grievances; in this case, taxpayer complaints. *Id.* at 348.

50. *See Clapper*, 133 S. Ct. at 1138 (using this foundational principle of standing to apply a rigorous standard of review to the particular set of facts presented before the court); United States v. Richardson, 418 U.S. 166, 188 (1974) ("Relaxation of standing requirements is directly related to the expansion of judicial power.").

51. The Court shows its hesitance to confer standing—particularly where a plaintiff challenges a government statute or action—where the harm is speculative. *See, e.g.*, *Richardson*, 418 U.S. at 176–77 (finding that plaintiff's lack of access to CIA spending records and his resulting inability to "properly fulfill his obligations as a member of the electorate" was a generalized grievance and insufficient to be considered an injury-in-fact); Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 220 (1974) (reaffirming the principle that standing cannot be predicated on an interest "which is held in common by all members of the public, because of the necessarily abstract nature of the injury all citizens share"); Laird v. Tatum, 408 U.S. 1, 13–14 (1972) (denying standing for plaintiffs—who argued that military program permitting surveillance of

This foundational principle mandating judicial wariness of speculative harms present one of the largest hurdles for data breach plaintiffs.[52]

To successfully bring a claim in federal court, a plaintiff must satisfy general Article III standing requirements.[53] The burden is on the plaintiff[54] to show: (1) that he has "suffered an 'injury in fact," i.e. "an invasion of a legally protected interested which is (a) concrete and particularized, and (b) actual or imminent, not 'conjectural' or 'hypothetical'";[55] (2) a causal connection between the injury and the conduct complained of—"the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court"; and (3) "it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'"[56] Each of the elements must be proven "with the manner and degree of evidence required at the successive stages of the litigation."[57] In the pleading stage, a court presumes the existence of the specific facts upon which a plaintiff's general factual allegations of injury rely.[58] To survive a summary judgment motion, a plaintiff must prove injury by pointing to specific facts.[59] In the class action context, plaintiffs representing

---

lawful and peaceful activity chilled the freedom of speech—because they did not present a threat of specific future harm or present objective harm); Baker v. Carr, 369 U.S. 186, 210 (1962) (noting that the nonjusticiability of "political questions" stems from the separation-of-powers principle).

52. *See infra* Part III.A (discussing cases where courts incorrectly apply this principle to deny standing even where speculation is minimal).

53. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013) ("Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'"). Standing is "one element of the case-or-controversy requirement." *Id.*

54. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) (requiring all plaintiffs seeking federal jurisdiction to establish all three elements of standing).

55. *See* Los Angeles v. Lyons, 461 U.S. 95, 101–02 (1983) (denying standing where plaintiff alleged an imminent injury stemming from a new police chokehold technique).

56. *See Lujan*, 504 U.S. at 560–61.

57. *Id.* at 561.

58. *See id.* (requiring courts to presume the existence of specific facts upon which a plaintiff's claim of injury relies in the pleading stage).

59. *See id.* (discussing the heightened burden of proof on plaintiffs at the summary judgment stage).

a class must show that they themselves have been personally injured; showing an injury to other members of the class is insufficient to confer standing for the named plaintiffs.[60]

B. Actual and Imminent Harm

An actual injury easily satisfies the injury-in-fact prong.[61] An imminent injury will occur in the future; the only question is, "how soon?" To establish standing, an injury-in-fact must be "'distinct and palpable'[62] as opposed to 'abstract.'"[63]A plaintiff can easily establish the injury-in-fact prong by pointing to an actual injury.[64] For example, the court in *Enslin v. Coca-Cola Company*[65] found that the plaintiff established a distinct and palpable actual harm by showing unauthorized credit card use, fraudulent withdrawals from bank accounts, and unauthorized issuances of credit cards after a series of laptop thefts.[66] Similarly, in *In re Target Corporation Data Security Breach Litigation*,[67] the court

60. *See* Lewis v. Casey, 518 U.S. 343, 357 (1996) (noting that plaintiffs cannot sue on behalf of a class if they themselves have not suffered an actual or imminent injury).

61. *See* Enslin v. Coca-Cola Co., No. 2:14-CV-06476, 2015 WL 5729241, at *14 (E.D. Pa. Sept. 30, 2015) (granting standing where plaintiffs suffered actual injuries stemming from laptop theft (citing Whitmore v. Arkansas, 495 U.S. 149, 155 (1990))).

62. *See* Warth v. Seldin, 422 U.S. 490, 501 (1975) (denying standing where plaintiffs sued a town for denying residence to low and moderate income individuals, finding that plaintiffs did not demonstrate that their immediate interests would be harmed without a favorable ruling).

63. *See* O'Shea v. Littleton, 414 U.S. 488, 494 (1974) (denying standing where plaintiffs alleged that racially discriminatory administration of the civil justice system deprived them of their constitutional rights, finding any future injury too abstract). *O'Shea* established the "real and immediate" standard that *Krottner* later uses to confer standing for imminent injury. *Id.* at 494.

64. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 (1992) (noting that for actual injuries, "the existence of standing is clear, though the precise extent of harm remains to be determined at trial").

65. 2015 WL 5729241.

66. *See id.* at *6 (distinguishing plaintiff's injuries from cases where the plaintiff had yet to be injured by a data breach). The stolen laptops contained the plaintiff's PII in an unencrypted state. *Id.*

67. 66 F. Supp. 3d 1154 (D. Minn. 2014).

granted standing where plaintiffs were subjected to fraudulent transactions on their credit cards.[68]

Imminent injuries are far less clear and are the source of myriad standing disputes in the data breach context.[69] To establish an "imminent" injury, there must be either a "substantial risk"[70] of future injury or the harm must be "certainly impending."[71] The two standards are not interchangeable and may possibly lead to different outcomes.[72] For example, the Court in *Whitmore v. Arkansas*[73] found that possible future injury is insufficient to confer standing; rather, the harm must be certainly impending.[74] In *Whitmore*, a plaintiff attempted to sue on behalf of a fellow inmate, arguing that the inmate's sentence could adversely affect his own sentencing.[75] The court denied standing, finding that any future injury was not certainly impending, given the difference of the inmates'

---

68. *See id.* at 1159 (conferring standing after a corporate server containing customer credit cards was breached and customers faced fraudulent transactions on their respective credit cards).

69. *See* cases cited *supra* notes 24–25 (listing relevant data breach law suits considering both actual and imminent harm).

70. *See* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–54 (2010) (finding that plaintiff alfalfa farmers established a "reasonable probability" that their organic alfalfa crops would be infected with an engineered gene—Roundup Ready Alfalfa—if it were completely deregulated). In *Monsanto*, the Court found a substantial risk of imminent harm because plaintiffs would, for example, be forced to continually test their organic alfalfa for contamination. *See id.* at 154 (finding that the resulting mitigation measures would create an irreparable harm justifying injunctive relief).

71. *See* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) (establishing that a threatened injury must be "certainly impending" and "allegations of *possible* future injury" are not sufficient).

72. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) (suggesting that the "substantial risk" standard set forth by *Monsanto Co. v. Geertson Seed Farms* is separate, distinct, and a lower threshold than the "certainly impending" standard set forth by *Whitmore v. Arkansas*).

73. 495 U.S. 149 (1990).

74. *See id.* at 158 ("A threatened injury must be 'certainly impending' to constitute an injury in fact." (citing Babbitt v. Farm Workers, 442 U.S. 289, 298 (1979))).

75. *See id.* at 159–60 (finding plaintiffs argument—that the inmates sentencing would immediately impact his own sentencing under Arkansas' comparative review in death penalty cases—unpersuasive, concluding that any future injury was not certainly impending).

respective crimes.[76] The Court in *Blum v. Yaretski*[77] granted standing where a threat was "sufficiently substantial."[78] In *Monsanto Company v. Geertson Seed Farms*,[79] the Court granted standing where there was a "substantial risk" of future harm.[80]

III. The Status of Data Breach Case Law

Before *Clapper*, there was well-established case law regarding imminent injury in data breach lawsuits.[81] This Note argues that *Clapper* does nothing to alter them.[82] The cases finding standing all implicitly focus on an unauthorized third party gaining access to unencrypted PII. The pre-*Clapper* cases suggest that a successfully carried out cyber-attack on a data network establishes a certainly impending injury.[83]

A. The Circuits' Slippery Slope

On August 23, 2007, the Seventh Circuit in *Pisciotta v. Old National Bancorp*[84] established what is likely the most lenient injury-in-fact requirement for standing in the data breach context.[85] The court found that a plaintiff must only show that defendants created an increased risk of future harm to establish

---

76. *See id.* at 157 (determining that a court's sentencing of a mass murderer was not similar enough to a robbery-murder for any injury to be certainly impending).

77. 457 U.S. 991 (1982).

78. *See id.* at 1000. The Court conferred standing where plaintiff—a member of a nursing home—faced the possibility of being transferred to a lower level of care. *Id.*

79. 561 U.S. 139 (2010).

80. *See supra* note 70 (discussing *Monsanto*).

81. *See infra* Part III.A (analyzing circuit court precedent that tends to lean in favor of data breach victims arguing imminent injury).

82. *See infra* Part V (arguing that the *Krottner* and *Pisciotta* standards remain forceful in light of a properly interpreted *Clapper*).

83. *See infra* Part V (arguing that this is the correct outcome).

84. 499 F.3d 629 (7th Cir. 2007).

85. *See id.* at 632 (granting standing in a "sophisticated, intentional and malicious" intrusion by hackers to Old National Bancorp's website).

standing.[86] In *Pisciotta*, defendant Old National Bancorp (ONB) ran a website where individuals applied for ONB's banking services.[87] Plaintiffs accessed the website in 2002 and 2004, respectively, providing various forms of PII.[88] In 2005, ONB's website hosting facility experienced a security breach that the court labeled as "sophisticated, intentional and malicious."[89]

The plaintiff's theory for standing relied on credit monitoring expenses incurred and similar future expenses resulting from the breach.[90] The plaintiffs did not, however, "allege any completed direct financial loss to their accounts."[91] The court was not persuaded by the more restrictive standing requirements district courts' followed in similar data breach contexts.[92] Rather, the court analogized this suit to toxic tort and medical malpractice

---

86. *See id.* at 634 (overturning the district court's dismissal for lack of standing).

87. *Id.* at 631.

88. *See id.* ("[S]ome forms require the customer or potential customer's name, address, social security number, driver's license number, date of birth, mother's maiden name and credit card or other financial account numbers.").

89. *Id.* at 632. It appears that the court attempted to use this as a factor to distinguish the present case from prior district court precedent denying standing. *See infra* note 92 (discussing cases denying standing where customer PII was misplaced or inadvertently stolen).

90. *See id.* at 631 ("[Plaintiffs] requested compensation for past and future credit monitoring services that they have obtained in response to the compromise of their personal data through ONB's website.").

91. *See id.* (stating that plaintiffs only needed to show an increase risk of injury, and the fact that the breach might cause greater harm in the future does "not affect the standing inquiry").

92. *See* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 7–8 (D.D.C. 2007) (denying standing where plaintiffs did not suffer actual harm from identity theft after an ING employee's personal laptop containing their PII was stolen in a home burglary). The court denied standing because plaintiffs did not allege that the laptop was stolen to access their PII or that their PII was even accessed. *Id.* The court determined that the injuries were founded on speculation and, therefore, insufficient to establish an imminent injury. *Id.*; *see also* Giordano v. Wachovia Sec., LLC., No. 06-476 JBS, 2006 WL 2177036, at *12 (D. N.J. July 31, 2006) (denying standing where a printed list containing plaintiff's PII was lost during shipping but did not result in harm to the plaintiff). The court denied standing because plaintiff failed to allege: (1) That the purpose of the burglary was to obtain her PII; (2) an actual injury; or (3) that she actually suffered identity theft. *Id.* at *5; *see also* Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (denying standing where an unauthorized access of customer PII occurred but plaintiff failed to allege that a third party intended to use her financial information or steal her identity).

suits, following the reasoning of several non-data breach sister circuit court opinions.[93] Consequently, the court found that a mere *increased risk* of harm was a cognizable injury sufficient to confer standing.[94]

On October 6, 2010, the Ninth Circuit in *Krottner v. Starbucks Corporation*[95] took *Pisciotta*'s lead.[96] In *Krottner*, thieves stole a laptop from a Starbucks location containing unencrypted names, social security numbers, and addresses of over 97,000 employees.[97] Plaintiffs were former Starbucks employees.[98] Starbucks notified all affected employees and advised them to monitor their credit as a precautionary measure.[99] Starbucks further provided one year of free credit monitoring service.[100] Plaintiffs' standing argument relied on the substantial amount of time and money spent to monitor their credit and the additional expenses that would arise after their complimentary credit monitoring expired.[101] One plaintiff further alleged that there was an unauthorized attempt in December 2008 to open a new bank account with his social security

---

93. *See* Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (noting, in dicta, that exposure to toxic substances could establish a risk of future harm sufficient to constitute an injury-in-fact); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (finding that a defective medical implant creates a increased risk of future harm sufficient to establish a cognizable injury); Cent. Delta Water Agency v. United States, 306 F.3d 938, 947–48 (9th Cir. 2002) (finding that possible future injury is sufficient to confer standing with regard to environmental harm); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000) (finding that increased risk of environmental harm is a cognizable injury sufficient to confer standing).

94. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) ("[T]he 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 harm that the plaintiff would've otherwise faced, absent the defendant's actions.").

95. 628 F.3d 1139 (9th Cir. 2010).

96. *See id.* at 1140 (conferring Article III standing, but ultimately affirming the lower court's dismissal of plaintiff's state-law claims).

97. *Id.*

98. *Id.*

99. *Id.* at 1141.

100. *See id.* (providing free credit monitoring even where Starbucks had no indication that the information was misused).

101. *See id.* (listing mitigation measures such as placing fraud alerts on credit cards and spending extra time monitoring 401(k) accounts).

number.[102] None of the plaintiffs suffered any financial loss in the form of identity theft.[103]

The Ninth Circuit found that one plaintiff's "generalized anxiety and stress" allegations were the only present injuries alleged.[104] These conferred standing for only one plaintiff.[105] With regard to the plaintiffs' future harms and mitigation argument, the court—much like *Pisciotta*—relied on *Century Delta Water Agency v. United States*.[106] It analogized an increased risk of identity theft to proposed governmental action creating a substantial risk of future harm in the environmental context.[107] Finding *Pisciotta* persuasive, the court established its own immediate injury standard: There is an injury-in-fact "if a plaintiff faces a 'credible threat of harm,'[108] the harm being 'both real and immediate, not conjectural or hypothetical.'"[109] The court found that the laptop theft created credible threat of real and imminent harm; most importantly, the court found that the harms were not conjectural or hypothetical—i.e. not speculative—

---

102. *Id.*

103. *Id.*

104. *Id.* at 1142. Standing requires *a plaintiff* to show harm; an injury to one party does not grant standing to the entire class. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992) ("[T]he *plaintiff* must have suffered an 'injury in fact' . . . ." (emphasis added)). "The 'injury in fact' test requires more than an injury to a cognizable interest. It requires that the *party seeking review be himself among the injured*." *Id.* at 563 (emphasis added).

105. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (relying on Supreme Court precedent to grant standing for anxiety caused by the potentially "'devastating' consequences" surrounding a possible disclosure of Social Security numbers (quoting Doe v. Chan, 540 U.S. 614, 617–18 (2004))).

106. *See* 306 F.3d 938, 947 (9th Cir. 2002) ("[T]he possibility of future injury may be sufficient to confer standing . . . threatened injury constitutes 'injury in fact.'").

107. *See id.* at 948 (finding standing for plaintiff farmers who established a substantial risk of their crops being destroyed by new governmental initiatives altering discharge of water from a reservoir). The court also analogized to cases of exposure to toxic chemicals where defendants failed to provide medical screening. *See* Pritikin v. Dept't of Energy, 254 F.3d 791,796–97 (9th Cir. 2001) (finding that defendant's failure to pay for plaintiff's medical screening after their exposure to toxic substances created a sufficient injury in fact).

108. *See generally* Cent. Delta Water Agency v. United States, 306 F.3d 950 (9th Cir. 2002) (finding standing where there was a substantial risk of irreparable environmental damage).

109. *See* Los Angeles v. Lyons, 461 U.S. 95, 102 (1983) (requiring a plaintiff to show a high degree of immediacy to confer standing).

because the laptop was already stolen.[110] Therefore, to the Ninth Circuit, theft of a laptop containing unencrypted PII created an imminent injury sufficient to confer standing. Until 2011, it appeared that similarly situated data breach victims had their foot in the door.[111]

And then came *Reilly v. Ceridian Corporation*.[112] On December 12, 2011, the Third Circuit filed its *Reilly* decision, denying standing and distinguishing itself from *Pisciotta* and *Krottner*.[113] The court followed an extremely restrictive standard that would deny standing in almost all data breach suits relying on imminent injury.[114] In *Reilly*, plaintiffs were Brach Eichler law firm (the Firm) employees.[115] The Firm was one of defendant Ceridian's—a payroll-processing firm—clients.[116] In December 2009, unknown hackers infiltrated Ceridian, potentially gaining access to customer PII.[117] It was inconclusive whether the hackers actually read, understood, or copied the data.[118] Ceridian sent letters to its customers informing them of their potential risk of identity theft and provided them with one year of free credit monitoring.[119] As a result, the plaintiffs filed a complaint against Ceridian alleging an increased risk of identity theft, credit

---

110. *See Krottner*, 628 F.3d at 948 (noting that, if the laptop had not been stolen and plaintiffs alleged an increased risk of future theft, the claim would be "far less credible").

111. The Ninth Circuit followed *Pisciotta*'s reasoning in reaching an identical conclusion earlier that same year. *See* Ruiz v. Gap, 380 F. App'x 689, 691 (9th Cir. 2010) (affirming the lower court in granting standing where thieves stole a laptop containing 750,000 job applicants" PII). At the district court level, it was unclear whether the laptops were stolen for their data or for their intrinsic value. Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 913 (N.D. Cal. 2009). Regardless, the court was persuaded by *Pisciotta* and district court precedent. *See id.* (granting standing for increased risk of future harm regardless of the thief's intentions (citing Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 276 (S.D.N.Y. 2008))).

112. 664 F.3d 38 (3rd Cir. 2011).

113. *See id.* at 44 (criticizing *Pisciotta* and *Krottner*'s standing analyses).

114. *See id.* at 43 (finding that injuries relying on actions by unknown third parties were too speculative to be considered imminent).

115. *Id.* at 40.

116. *Id.*

117. *See id.* (noting that the stolen PII included first and last names, social security numbers, and in some cases, birthdays and bank account numbers).

118. *Id.*

119. *Id.*

monitoring costs to mitigate the alleged risk, and emotional distress.[120]

The Third Circuit denied standing on the plaintiffs' increased risk of identity theft argument for three reasons. First, the plaintiffs' standing theory relied on a speculative chain of events, thereby failing to show an injury with a high degree of immediacy.[121] To the court, the fact that hacker had to read and understand the PII, intend to use it to the plaintiffs' detriment, and actually make unauthorized harmful transactions created an impermissible level of speculation.[122] The court could not find an explanation for any future injury without beginning with the word "if" and, as such, found the injury to be too speculative.[123] Second, the court found the plaintiffs' reliance on *Pisciotta* and *Krottner* unpersuasive.[124] This was predominantly because the plaintiffs in the present case neither pleaded a "sophisticated, intentional and malicious"[125] intrusion nor alleged any misuse of their PII—i.e. no actual injury.[126]

Third, persuaded by district courts, the court refuted *Pisciotta*'s constitutional standing analysis altogether and distinguished the present case from *Krottner*.[127] In discrediting the *Pisciotta* analysis, the court determined that *Pisciotta*

---

120. *Id.*

121. *See id.* at 42 (mandating the immediacy requirement as essential to preventing the court from ruling on an injury that may never occur (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 n.2 (1992))).

122. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3rd Cir. 2011) (requiring this chain of events to produce an injury before plaintiffs had standing, therefore, effectively eliminating imminent injury as an option for data breach plaintiffs).

123. *See id.* at 43 (emphasizing that that, in a prior case, the court denied standing because plaintiffs could not allege how they "will be injured without beginning the explanation with the word 'if'" (quoting Storino v. Borough of Point Pleasant Beach, 322 F.3d 293, 297–98 (2003))).

124. *See id.* at 44 (distinguishing the circumstances between the present case and *Pisciotta* and *Krottner*).

125. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (finding standard).

126. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing).

127. *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d. 1046, 1051–53 (E.D. Mo. 2009) (ruling that the risk of future harm posed by future data theft in which the harm may occur is too speculative); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006) (same).

incorrectly analogized data breach to toxic torts, defective medical devices, and environmental harm.[128] Importantly, in the court's eyes, injury already occurred in medical-device and toxic exposure cases.[129] The court opined that the only question left in such cases is to what extent or how the injury will manifest, whereas in data breach, the plaintiff's status quo has not changed.[130] Also, data breach cases do not "hinge on human health concerns."[131] The court notes a clear distinction and accompanying willingness for courts to confer standing when human injury may occur rather than mere monetary harm.[132] The court also discounted the environmental harm analogy because monetary compensation cannot repair environmental damage, but it can make a credit fraud victim whole.[133] It reasoned that mere monetary damages could be recouped once incurred and the calculations could be more precise.[134] But, before any damages occurred, they were entirely speculative.[135]

Finding that the harms were purely speculative, the court determined that the plaintiffs' resulting mitigation costs did not

---

128. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3rd Cir. 2011) (discussing the *Pisciotta* court's failure to address the "imminent" and "certainly impending" requirements altogether).

129. *See* Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (noting, in dicta, that exposure to toxic substances could establish a risk of future harm sufficient to constitute an injury-in-fact); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (finding that a defective medical implant creates a increased risk of future harm sufficient to establish a cognizable injury).

130. *See Reilly*, 664 F.3d at 45 (noting that any future harm is not quantifiable in data breach, whereas in toxic torts, a significantly heightened risk of bodily harm is imminent). In *Reilly*, the plaintiff's status was the same as if the breach never occurred. *Id.*

131. *Id.*

132. *See id.* ("The deceased, after all, have little use for compensation. This case implicates none of these concerns.").

133. *See id.* (recognizing that monetary damages may not be adequate in the context of environmental harm (citing Cent. Delta Water Agency v. United States, 306 F.3d 938 (9th Cir. 2002))).

134. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 44–46 (3rd Cir. 2011) (failing to recognize that injuries occurring several years after a breach would be increasingly difficult to trace to the defendants).

135. *See id.* (noting that the identity theft may never occur and speculating what damages may occur cannot be accurately calculated).

result from a cognizable injury-in-fact.[136] The court found that mitigation costs "protect[ing] against an alleged increased risk of identity theft [are] not enough to demonstrate a concrete and particularized or actual or imminent injury."[137] Because plaintiffs' mitigation costs were not incurred in fear of a certainly impending injury, the costs were no more an actual injury than the alleged future harms.[138] To the *Reilly* court, an impermissible level of speculation exists between the hackers viewing private PII and hackers actually using it to a plaintiff's detriment.

Fortunately, the First Circuit at least set a minimum threshold requirement. In 2012, the First Circuit in *Katz v. Pershing, LLC*[139] recognized a common thread among the circuits: hackers actually accessed the data in all three cases.[140] The court acknowledged access to data as the very minimum and as such, denied standing where the plaintiff claimed an increased risk of *access* to her PII.[141] In *Katz*, the plaintiff argued that the defendant's investment services, which gave "end users" unfettered access to her PII, left it inadequately protected.[142] These end users were people, such as investment consultants, working for the customers' benefit.[143] The court implicitly limited *Pisciotta*'s generalized increased risk of harm standard when it denied standing.[144] While *Katz* recognized *Pisciotta*'s, *Krottner*'s,

136. *See id.* at 46 (finding that mitigation costs incurred by the plaintiffs' reliance on a speculative or hypothetical harm were done merely to ease their fears and not a reasonable response to the given circumstances).

137. *Id.* (internal citations omitted).

138. *See id.* ("[Plaintiffs] prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent.").

139. 672 F.3d 64 (1st Cir. 2012).

140. *See id.* at 80 (reading *Pisciotta*, *Krottner*, and *Reilly* to require, at a very minimum, that a plaintiff plead actual unauthorized access to PII). "In each of the[se cases], the plaintiffs' data actually had been accessed by one or more unauthorized third parties." *Id.*

141. *See id.* ("[T]he plaintiff alleges only that there is an increased risk that someone might access her data and that this unauthorized access (if it occurs) will increase the risk of identity theft and other inauspicious consequences . . . . This omission is fatal . . . .").

142. *Id.* at 70.

143. *Id.* at 69.

144. *See id.* (requiring actual access, the court implicitly tightened *Pisciotta*'s extremely broad standard). Recall, *Pisciotta* states that "the injury-

and *Reilly*'s inconsistencies, its import is clear: at a bare minimum, the plaintiff needed to plead *unauthorized access* to her PII.

B. Clapper v. Amnesty International USA

On February 26, 2013, the Supreme Court announced *Clapper v. Amnesty International USA*,[145] a seminal case on Article III standing that some courts interpret as the modern test for imminent injury.[146] In *Clapper*, the Court found that the plaintiffs' allegation of future harms and the ensuing mitigation costs were based on a chain of events too speculative to be considered "certainly impending."[147] The plaintiffs were attorneys and human rights organizations[148] working with clients that, they argued, were likely targets of surveillance under the Foreign Intelligence Surveillance Act (FISA) Amendments Act (the Act).[149] The Act grants the Executive Branch the authority to intercept foreign communications.[150] Plaintiffs, without any proof of the government intercepting their communications, sought a

---

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 harm that the plaintiff would have otherwise faced, absent the defendant's actions*." Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629, 634 (7th Cir. 2007) (emphasis added). The plaintiff arguably would have satisfied *Pisciotta*'s concededly loose standard.

145. 133 S. Ct. 1138 (2013).

146. *See infra* Parts V (arguing that this is an inappropriate interpretation).

147. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013). *See* Whitmore v. Arkansas, 495 U.S. 149, 158 (1990) ("Allegations of possible future injury do not satisfy the requirements of Art. III. A threatened injury must be 'certainly impending' to constitute injury in fact." (citing Babbitt v. Farm Workers, 442 U.S. 289, 298 (1979))).

148. *See Clapper*, 133 S. Ct. at 1145 (noting that plaintiffs clients are located in areas likely to be targeted by FISA).

149. *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885(c) (2012) (authorizing and regulating certain governmental electronic surveillance of communications for foreign intelligence purposes).

150. FISA permits the President, through the Attorney General, to "authorize electronic surveillance . . . solely directed at . . . the acquisition of . . . communications used exclusively between or among foreign powers." *Id.* § 1802(a). The Attorney General must obtain the Foreign Intelligence Surveillance Court's approval. *Id.* § 1881(g). The Act permits "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." *Id.* § 1881(a).

declaration finding § 1881a unconstitutional and permanently enjoining against its use.[151] The plaintiffs claimed that § 1881a of the Act "compromise[d] their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[152] The plaintiffs further claimed that the Act forced them to incur considerable expenses traveling to their clients to communicate in person.[153]

The plaintiffs raised two standing theories: (1) there was an "objectively reasonable likelihood" an injury would occur because their communications would be intercepted in the future;[154] and (2) the risk of surveillance under the Act was so substantial that the mitigation costs incurred to prevent it "constitute [a] present injury . . . fairly traceable to § 1881a."[155]

The district court denied standing.[156] The only issue on appeal to the Second Circuit was whether the plaintiffs could legally assert their claims in federal court.[157] The Second Circuit reversed the district court's decision, finding an "objectively reasonable likelihood" that the plaintiffs' future communications would be intercepted "at some time in the future."[158] The court further found that the plaintiffs suffered present injuries

---

151. The entirety of the plaintiffs' complaint sought "(1) a declaration that §1881a, on its face, violates the Fourth Amendment, the First Amendment, Article III, and separation-of-powers principles and (2) a permanent injunction against the use of §1881a." *Clapper*, 133 S. Ct. at 1146.

152. *Id.* at 1145.

153. *See id.* at 1145–46 (characterizing the plaintiffs mitigation efforts to "protect the confidentiality of sensitive communications" as "costly and burdensome").

154. *Id.* at 1146. The Court also found the Second Circuit's standard too lax to satisfy traditional standing requirements. *See id.* at 1141 ("[T]he Second Circuit's "objectively reasonable likelihood" standard is inconsistent with this Court's "threatened injury" requirement.").

155. *Id.* at 1146.

156. *See* Amnesty Int'l U.S. v. McConnell, 646 F. Supp. 2d 633, 645 (S.D.N.Y. 2009) (finding "fear of surveillance" to be an "abstract fear" and therefore, insufficient to confer standing). The court also denied the plaintiffs' standing for mitigation costs incurred resulting from the alleged fear of surveillance. *Id.* at 652.

157. *See* Amnesty Int'l U.S. v. Clapper, 638 F.3d 118, 121 (2d Cir. 2011) (noting that the court was not answering the question of whether the claims were valid).

158. *Id*. at 118.

stemming from the reasonable fear of future harm.[159] The Supreme Court granted certiorari to answer two specific questions: whether the plaintiffs had Article III standing to challenge the constitutionality of § 1881a and whether it should permanently enjoin the government from authorizing surveillance under § 1881a.[160]

Importantly, the Court applied an *elevated* standing inquiry.[161] This "especially rigorous" standing inquiry applies where a dispute forces the Court to decide on the constitutionality of Executive or Legislative action.[162] The Court has traditionally denied standing in cases involving government actions in federal intelligence gathering.[163] With this heightened standard in mind, the Court analyzed the plaintiffs' claims of future harms and mitigation costs, which relied on possible actions by the Legislative and Executive Branches.[164]

The Court considered several factors.[165] First, the plaintiffs provided no evidence of intercepted communications under the

---

159. *See id.* at 138 ("Because standing may be based on a reasonable fear of future injury and costs incurred to avoid that injury, and the plaintiffs have established that they have a reasonable fear of injury and have incurred costs to avoid it, we agree that they have standing.").

160. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1142 (2013) (discussing whether plaintiffs claim of future harm could be classified as "certainly impending" (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))).

161. *See id.* at 1147 (acknowledging that Article III standing serves as a check on the judiciary "to prevent the judicial process from being used to usurp the powers of the political branches" (citations omitted)); *infra* Part III.C (discussing cases where this critical distinction was ignored).

162. *See Clapper*, 133 S. Ct. at 1142 (justifying the Court's rigorous review to prevent the expansion of judicial power in cases affecting the separation of powers).

163. *See* United States v. Richardson, 418 U.S. 166, 180 (1974) (finding that plaintiffs needed more than "generalized grievances" to establish standing when contesting a statute permitting the Central Intelligence Agency to account for its expenditures solely on the certificate of the CIA Director); Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 220–21 (1974) (requiring the plaintiffs to actually be harmed to have standing to challenge the Armed Forces Reserve membership of Members of Congress); Laird v. Tatum, 408 U.S. 1, 15–16 (1972) (finding fear of surveillance insufficient to confer standing to challenge an Army intelligence-gathering program).

164. *See Clapper*, 133 S. Ct. at 1147 (stating that the Court traditionally does not confer standing when the decision would review the actions of other political branches).

165. The plaintiffs needed to either establish an actual harm or allege a

Act.[166] The plaintiffs merely claimed that the Act would harm them in the future.[167] Second, the plaintiffs' theory for future harms relied on a speculative chain of events.[168] A series of five events needed to occur before the plaintiffs' confidential communications were intercepted: (1) the government must choose to target plaintiffs' clients;[169] (2) the government must opt for surveillance under § 1881a;[170] (3) the judge serving on the Foreign Surveillance Court must find the government's request satisfactory in light of the requirements under §1881a;[171] (4) the government must succeed in actually acquiring the plaintiffs' contacts' communications;[172] and (5) the plaintiffs must be parties

---

harm that was certainly impending. *See supra* Part II (discussing these requirements as the constitutional minimum).

166. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013) (noting that the plaintiffs filed suit on the day when the Act was passed—they were not yet harmed).

167. Plaintiffs' claim relied largely on the assumption (with little knowledge as to the government's targeting practices) that government officials would target their clients under § 1881a. *See id.* at 1148 (relying on assumptions that communications *may* be intercepted in an attempt to classify mitigation costs as harms sufficient to confer standing).

168. The *Whitmore* Court implicitly accepted that imminence claims require a certain degree of speculation; however, certain claims are *too* speculative. *See* Whitmore v. Arkansas, 495 U.S. 149, 157 (U.S. 1990) (finding, under Arkansas' comparative review of death penalty sentencing, that a sentencing for a mass murderer was not similar enough to that of a robbery-murder to create an imminent injury—any injury was "too speculative").

169. *See Clapper*, 133 S. Ct. at 1148–49 (2013) (finding that, because the plaintiffs have no "actual knowledge of the Government's targeting practices," they, at best, could "merely speculate and make assumptions about whether their communications" would be intercepted). Article III standing cannot rest on "'mere allegations,' but must be 'set forth' by affidavit or other evidence 'specific facts.'" *Id.* (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 561 (1992)). The plaintiffs had no knowledge of the government's practices, and therefore, they could not provide—nor had they provided—concrete evidence that their clients would be targeted. *See id.* at 1149 (finding that plaintiffs' lack of knowledge regarding governmental discretion under the Act can only lead to speculation).

170. *See id.* at 1149 (finding that, even if plaintiffs could prove that interception of their communications was imminent, they would not be able to trace them back to the Act, thereby failing the "fairly traceable" prong for Article III standing).

171. *See id.* at 1150 ("[R]espondents can only speculate as to whether that court will authorize such surveillance."); Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a(f)–(g) (2012) (establishing guidelines for compliance and certification requirements).

172. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 (2013) (noting

to the intercepted communications.[173] Based on this speculative chain of events, the Court found that the plaintiffs' injuries were neither certainly impending nor fairly traceable to the Act.[174]

The speculative chain of events proved fatal to plaintiffs' second theory for standing.[175] The Court dismissed the plaintiffs' argument that the Act created ongoing injuries requiring the plaintiffs to undertake costly mitigation measures.[176] The Court refused to follow the Second Circuit's "relaxed reasonableness standard."[177] As a result, it found that mitigation costs must stem from a certainly impending threat.[178] Because the threat was not certainly impending, the mitigation costs were not a "reasonable reaction to a risk of harm."[179] Therefore, without a certainly impending threat, the mitigation costs were merely an attempt to "manufacture standing" rather than an actual injury.[180]

Essentially, dismissal of the plaintiffs' first argument[181] proved fatal to the second.[182] The Court found that any alleged

---

that the Government's efforts to intercept plaintiffs' communications is not guaranteed).

173. *See id.* (determining that plaintiffs could only "speculate as to whether their own communications with their foreign contacts would incidentally be acquired").

174. The Court, however, acknowledged that plaintiffs can establish standing if there is a "substantial risk" that harm will occur. *Id.* at 1150 n.5 (citing Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2754–55 (2010)). Plaintiffs "fall short of even that standard." *Id.*

175. *See id.* at 1151 (finding that mitigation costs not related to an imminent injury are insufficient to confer standing).

176. *See id.* (denying standing because plaintiffs inflicted harm upon themselves without the presence of a certainly impending threat).

177. *See id.* at 1148 (refusing to follow the Second Circuit's "objectively reasonable likelihood" theory because it was too loose and, therefore, inconsistent with the requirement that "'threatened injury must be certainly impending to constitute injury in fact.'" (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))).

178. *See id.* (finding that, because the threat was found not to be certainly impending, the mitigation costs were merely the result of an unwarranted fear of surveillance and, therefore, insufficient to confer standing).

179. *Id.* at 1151.

180. *See id.* (noting that, because the threat was too speculative to be considered certainly impending, plaintiffs' mitigation costs were unreasonable and insufficient to establish standing (citing Pennsylvania v. New Jersey, 426 U.S. 660, 664 (1976))).

181. *See id.* at 1146 (arguing that an injury would occur because there was an "objectively reasonable likelihood" that their communications would be

future harm relied on a speculative chain of events and concluded that the alleged injury was not certainly impending.[183] Mitigation costs cannot stem from a hypothetical future harm.[184] Therefore, the Court found that the plaintiffs used mitigation costs as a way to manufacture standing.[185]

C. The District Courts Follow Suit

Many district courts interpret *Clapper* as a large hurdle for data breach claims relying on imminent injury;[186] others interpret *Clapper* to tighten constitutional standing altogether.[187] While *Clapper* was concerned with the narrow and constitutionally sensitive subject of foreign surveillance under FISA, courts have applied it to a broad range of standing issues, including data breach cases.[188]

---

intercepted in the future).

182. *See id.* (arguing that the risk of surveillance under the Act was so substantial that the mitigation costs incurred to prevent it "constitute [a] present injury that is fairly traceable to § 1881a"). The Court concluded that "allowing respondents to bring th[e] action based on costs they incurred in response to a speculative threat would be tantamount to accepting a repackaged version of respondent's first failed theory of standing." *Id.* at 1151.

183. *See id.* at 1143 ("[R]espondents' theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'" (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990))).

184. *See id.* (noting that, if standing could be based on mitigation costs extending from a hypothetical future harm, a plaintiff could merely purchase a plane ticket and have standing to sue).

185. *See id.* ("[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending.").

186. *See, e.g.*, *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (following *Clapper* correctly, finding that "there were simply too many 'ifs' involved before an injury came to pass").

187. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) (discarding past data breach precedent in light of *Clapper*, essentially foreclosing *any* imminence claim for data breach victims).

188. *See infra* notes 189–247 (discussing the cases that interpret *Clapper* as a virtual ban on imminent injury in data breach case law).

On September 3, 2013, the Northern District of Illinois, in *In re Barnes & Noble Pin Pad Litigation*,[189] properly applying *Clapper*, denied standing where the plaintiffs suffered no actual injury from pin pad "skimming" at sixty three of defendant's stores.[190] The plaintiffs argued an increased risk of identity theft, resulting anxiety, emotional distress, as well as mitigation costs.[191] The court noted the potential market for the stolen credit card numbers, recognizing that some could be sold for as little as $1.50 or as much as $90.00.[192] The court found that the plaintiffs failed to plead concrete facts showing actual harm.[193] Interestingly, the court did not find an actual injury even where a plaintiff faced a reimbursed fraudulent charge; it believed that the only way a defendant could suffer an actual injury was though an "*unreimbursed* charge on her credit card."[194] Here, she only claimed loss of credit card use and it was not directly apparent whether any unauthorized charges were related to the breach.[195]

The court, citing *Clapper*, denied the plaintiffs' alleged increased risk of identity theft and mitigation cost claims.[196] The plaintiffs could not prove that their information was actually stolen; therefore, the claim was more akin to increased risk of

---

189. No. 12-CV-8617, 2013 WL 4759588 (N.D. Cal. Mar. 3, 2013).

190. *See id.* at *2–3 (describing "skimming" as the process of reading and extracting temporarily stored credit card data from physical in-store pin pads used by customers to make payments).

191. *See id.* at *7–12. (finding that these claims did not satisfy the certainly impending standard reaffirmed in *Clapper*). Importantly, the court noted *Clapper*'s recognition of a less rigorous standing inquiry. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) ("[W]e have found standing based on a 'substantial risk' that the harm will occur.").

192. *Barnes & Noble Pin Pad*, No. 12-CV-8617, 2013 WL 4759588, at *4.

193. *Id.* at *8 (finding that loss of credit card use was not an actual injury).

194. *Id.* at *16 (emphasis added).

195. *Id.* Without proving that hackers actually accessed the data, it becomes increasingly difficult to trace the plaintiffs' injuries to the pin pad skimming. *See id.* at *12 (denying any actual injury because the plaintiffs did not plead the necessary facts to establish that their PII was stolen).

196. *Id.* at *11–12. As we saw in *Katz,* plaintiffs cannot allege an increased risk of *access*; a legitimate imminence theory requires at least access to PII. *See* Katz v. Pershing, 672 F.3d 64, 80 (1st Cir. 2012) (reading the Seventh Circuit's increased risk of harm theory to exclude an increased risk of access that would later lead to possible future harm).

access rather than harm.[197] Accordingly, the inherent speculation also discredited the plaintiffs' mitigation argument.[198] The court's hesitation to grant standing based on *Clapper* was justified; unlike a network breach, it is difficult to show that the plaintiff used the particular pin pad that was targeted. So, even if the plaintiffs shopped in an affected store, future harm would rely on proof that *the particular* pin pad was hacked.[199] But, much to the chagrin of data breach victims, other district courts deny standing even when hackers have possession of the PII.[200]

On February 10, 2014, the Southern District of Ohio in *Galaria v. Nationwide Mutual Insurance Company*[201] interpreted *Clapper* as heightening the imminence standard for data breach plaintiffs. The facts are familiar: the plaintiffs gave their PII—such as names, addresses, social security numbers—to apply for insurance, then the network containing this information was hacked.[202] Defendant insurance company, which provided one year of free credit monitoring, instructed the plaintiffs to monitor their credit, and suggested they freeze their credit cards at their own expense.[203] The plaintiffs' PII was neither misused nor were their identities stolen.[204] Among other claims, the plaintiffs

197. *See In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, *12 (N.D. Cal. Mar. 3, 2013) ("Plaintiffs 'cannot manufacture standing by incurring costs in anticipation of non-imminent harm.'" (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013))). It is important to note that the pin pad skimming must have occurred in person at the store; this was not a hacking of a network. *Id.* at *2–3. The plaintiffs did not allege that the particular store they shopped at was breached; they were merely "customers during the time when the skimming occurred." *Id.* at *3.

198. *See id.* at *11–12 (denying mitigation costs because they were not in response to an imminent harm).

199. *See id.* at *2 (creating a high level of speculation because the plaintiffs' argument assumed that, out of Barnes and Nobles' 700 stores, the thieves "skimmed" the particular pin pad that they used).

200. *See infra* notes 201–244 and accompanying text (discussing cases interpreting *Clapper* to essentially foreclose any imminence argument in the data-breach context).

201. 998 F. Supp. 2d 646 (S.D. Ohio, Feb. 10, 2014).

202. *Id.* at 650.

203. *See id.* (admitting that the plaintiffs' information was actually stolen and disseminated).

204. *Id.*

alleged increased risk of harm—including identity theft, identity fraud, or medical fraud—and associated mitigation costs.[205]

The court denied standing, finding the plaintiffs' position similar to that of respondents' in *Clapper* and refused to follow *Pisciotta* and *Krottner*.[206] Importantly, the court conceded that the hackers might have the plaintiffs' PII in their possession; however, it misinterpreted *Clapper*, finding that all claims relying on third-party behavior as speculative.[207] The court opined that any future harm was contingent on the actions of third parties and therefore, speculative.[208] However, the *Clapper* Court was reluctant to pass judgment on actions taken by *government actors* in light of an "especially rigorous" standing inquiry.[209] *Clapper* is not a complete ban on standing, especially when hackers have possession of plaintiffs' PII. The only step left for plaintiffs to be injured is actual identity theft, credit fraud, etc.[210]

---

205. *See id.* at 651 (citing *Pisciotta*'s standard as applicable and analogous to their case).

206. *See supra* notes 84–110 and accompanying text (finding an increased risk of future injury or real and immediate threat of future harm sufficient to confer standing where laptops containing plaintiffs' PII were stolen).

207. *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) ("Named Plaintiffs received a letter from Defendant indicating that on October 23, 2012, thieves hacked into a portion of Defendant's computer network and that their PII was *stolen and disseminated* as part of the theft." (emphasis added)).

208. *See id.* at 655 ("[T]he Supreme Court is reluctant to find standing where the injury-in-fact depends on the actions of independent decision-makers as the injury in those circumstances is speculative." (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1141 (2013))).

209. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1141 (2013) (applying this heightened standard in light of separation-of-powers concerns).

210. The *Adobe* and *Remijas* courts apply this very reasoning. *See* Remijas v. Neiman Marcus Grp, LLC, 794 F.3d 688, 696 (7th Cir. 2015) (finding that, once data thieves obtained unencrypted customer data, victims should not have to wait for an actual injury to occur before having standing to sue—the breach created a "substantial risk" of future identity theft); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. Sept. 4, 2014) ("[R]equir[ing] Plaintiffs to wait until they actually suffer identity theft or credit card fraud . . . would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact.").

Most importantly, the court did not follow circuit precedent—*Pisciotta*, *Krottner*, and *Ruiz v. Gap*[211]—because of *Clapper*. The court stated that these cases "were decided prior to *Clapper* . . . . [Which] specifically rejected the idea that an injury is certainly impending if there is an 'objectively reasonable likelihood' it will occur."[212] It essentially saw the objectively reasonable likelihood standard as synonymous with the Ninth Circuit's increased risk of future harm standard and, as such, found that *Clapper* overruled it.[213] The court determined that "the increased risk of harm may satisfy the [Ninth Circuit's] standards, but under *Clapper*, more is required to show an injury is certainly impending."[214]

In sum, the court took *Clapper* to reject the Ninth Circuit's increased risk of future harm standard and chose to follow *Reilly*[215] and several district courts.[216] Because the harm was not imminent, the mitigation costs were based on speculation, and therefore, they were merely a way to "manufacture standing."[217] However, not all courts apply *Clapper* with a broad brush, and the next case exemplifies the tension between existing data breach case law and *Clapper*'s reiteration of the certainly impending standard.

---

211. 380 F. App'x 689, 691 (9th Cir. 2010). For a brief discussion on *Ruiz*, see *supra* note 111 (finding standing where laptops containing PII were stolen).

212. *Galaria*, 998 F. Supp. 2d at 656 (S.D. Ohio 2014).

213. *See id.* at 654 (interpreting *Clapper*'s overruling of the Second Circuit's "objectively reasonable likelihood" standard to foreclose any future injury that is not certainly impending).

214. *See id.* at 656 (discounting *Krottner*'s standing requirement as too loose in light of *Clapper*).

215. The court's reliance on *Reilly* is improper as well. In *Reilly*, there was no indication that the plaintiffs' information was even stolen or viewed, whereas here, defendants conceded that the plaintiffs' PII was in fact stolen. *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) ("[T]heir PII was stolen and disseminated as part of the theft.").

216. *See id.* at 657 ("[T]he Court finds persuasive the reasoning in the line of cases rejecting risk of harm as an injury-in-fact in the context of data breaches.").

217. *See id.* ("'[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." (citing Clapper v. Amnesty International USA, 133 S. Ct. 1138, 1151 (2013))).

"[T]he import of *Clapper* for standing analysis in the Seventh Circuit . . . is a question on which reasonable minds may differ."[218] Relegated to a footnote, the Northern District of Illinois in *Strautins v. Trustwave Holdings, Inc.*[219] not only acknowledged *Clapper*'s special circumstances, but also recognized the substantial risk standard.[220] It did not, however, place enough emphasis on *Clapper*'s difficult constitutional context.[221] The *Strautins* court dealt with a large-scale breach of South Carolina's Department of Revenue; the allegations were against the employed data-security service—Trustwave—for an "imminent, immediate and continuing increased risk of identity theft and identity fraud."[222] The defendants announced that some taxpayers were *potentially* compromised and provided free services to determine if the plaintiffs in particular were affected.[223] The plaintiff neither received notice that her data was compromise nor did she take advantage of the free services.[224] The court correctly dismissed for lack of standing, and it is easy to see why.[225] However, the same conclusion could have arguably been reached applying *Pisciotta*.[226]

---

218. Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 n.11 (N.D. Ill. 2014). As we will see, the Seventh Circuit in *Remijas* provides the answer. *See infra* Part IV (limiting *Clapper* to the narrow context of theories of future injury relying on the actions of independent government actors).

219. 27 F. Supp. 3d 871 (N.D. Ill. 2014).

220. *See id.* at 878 n.11 (acknowledging that standing formulations vary and that the court has in the past applied less rigorous standards in different contexts).

221. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1146 (2013) ("The law of Article III standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches.").

222. *See Strautins*, 27 F. Supp. 3d at 874 (noting, importantly, that South Carolina provided a website helping users find out if they were affected and also offered free credit monitoring and a lifetime of credit resolutions).

223. *See id.* ("[T]he state set up a website and toll-free hotline for taxpayers to determine if their data was compromised.").

224. *See id.* ("Strautins admits that she . . . never used the website.").

225. South Carolina provided an online service to determine if a taxpayer's specific PII was in fact compromised. *Id.* The plaintiffs did not use the online service and could not prove that their particular PII was even compromised. *Id.*

226. The plaintiff's entire argument relied solely on the fact that because she was once a taxpayer in South Carolina, then her PII must have been stolen. *Id.* at 880. The court found, however, that the breach "did *not* result in the

As a district court in the Seventh Circuit, however, the court found that *Clapper* completely overruled *Pisciotta*.[227] The court felt "duty bound" to follow *Clapper* because both cases involved "potential unauthorized disclosure of sensitive personal information."[228] Ultimately, the court found that standing was not the controlling issue because Strautins "failed even to plausibly allege that her PII was stolen."[229] This is significant because the court could have left *Pisciotta* entirely untouched, but it instead it boldly asserted that *Clapper* overruled the established Seventh Circuit precedent for data breach suits.[230]

Clapper's unique set of facts should not, however, be construed to disqualify its application entirely. *Clapper* denies standing where future injury relies on a truly speculative chain were to occur.[231] A *highly* speculative chain of events, under *Clapper*, *should* overcome a plaintiff's future injury claim.[232] On

---

compromise of data of all taxpayers filing . . . since 1998." *Id.* at 881 (emphasis added). Even applying the increased risk of future injury standard in *Pisciotta*, the plaintiff provided no evidence to show that she is part of the class affected by the breach. *See id.* at 874 (emphasizing that the plaintiff neither received a notice that her information was stolen nor did she check the South Carolina website). The plaintiff's case certainly would not satisfy *Katz*. *See supra* notes 139–144 and accompanying text (noting *Katz* required the plaintiff to at least show *access* to her PII).

227. *See* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 (N.D. Ill. 2014) ("Clapper seems rather plainly to reject the premise, implicit in Pisciotta . . . that any marginal increase in risk is sufficient to confer standing.").

228. *Id.* at 879. The *Strautins* court failed to consider the distinct difference between the two cases. *See infra* Part V.A.1 (urging that *Clapper* was not a data breach case and its application in the data breach context should be limited).

229. *See Strautins*, 27 F. Supp. 3d at 879 n.11 (finding that the plaintiff "failed to establish even the *proposition* that she is at an increased risk of identity theft" (emphasis added)). While the court did not cite to it, this is the exact application of the First Circuit baseline standard. *See* Katz v. Pershing, 672 F.3d 64, 80 (1st Cir. 2012) (denying standing for increased risk of access).

230. *See Strautins*, 27 F. Supp. 3d at 879 n.11 ("[T]his Court cannot square [*Pisciotta*] with *Clapper*."). The court likened the Second Circuit's "objectively reasonable likelihood" standard to *Pisciotta*'s "increased risk of harm." *Id.* Because *Clapper* explicitly declined to follow the Second Circuit standard as too loose, the court believed that it must have also overruled *Pisciotta*'s standard. *Id.*

231. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) ("[R]espondents' argument rests on their highly speculative fear . . . .").

232. Imminence theories relying on speculative chains of events have traditionally been dismissed for lack of standing; *Clapper* was merely following

May 9, 2014, the District Court for the District of Columbia in *In re Science Applications International Corporation (SAIC) Backup Tape Data Theft Litigation*[233] did just that. SAIC is an information technology company that handles data for the federal government.[234] In what appeared to be a typical car theft, a SAIC employee's car was broken into and the thief stole the stereo, GPS system, and several data tapes.[235] Those data tapes, however, contained the PII—including medical records—of 4.7 million military members.[236] Plaintiff military members argued that an increased risk of harm alone was sufficient to establish standing.[237] The court, relying on *Clapper*, dismissed the cases because of the highly speculative chain of events required before any injury transpired or the data was even accessed.[238]

As in *Clapper*, the increased risk of future identity theft was truly speculative. Assuming that the person who stole the tapes was just a run-of-the-mill car thief, he would have to: (1) recognize that the tapes contained computer readable PII, as opposed to what would be found in a typical car tape-deck; (2) find a data-tape reader and connect it to his computer; (3) download software to upload the tapes—or otherwise, slowly spool it through similar cassettes to obtain the data; (4) decrypt the portions of encrypted data; (5) acquire familiarity with the database format, and; (6) misuse or sell it.[239] The fact that the tapes could either be in a landfill or fully uploaded to the thief's computer was simply too speculative to constitute an increased threat of identity theft, let alone a certainly impending injury.[240]

---

precedent. *See, e.g.*, Whitmore v. Arkansas, 495 U.S. 149, 159–60 (1990) (denying standing where a plaintiffs injury relied on obtaining habeas relief, a retrial, a reconviction, and a death sentence).

233. 45 F. Supp. 3d 14 (D.D.C. May 9, 2014).

234. *Id.* at 19. The tapes contained only personal information and no credit card numbers. *Id.* at 20.

235. *See id.* (implying that the thieves most likely stole the tapes for their intrinsic value rather than for their information).

236. *Id.*

237. *Id.*

238. *See id.* at 25 (finding plaintiffs' argument, that they were 9.5 times more likely to become victims of identity theft, unpersuasive in light of *Clapper* because *Clapper* requires more than an increased risk of harm).

239. *Id.*

240. *See id.* at 25–26 (implicitly focusing on the fact that the burglars, more

However, after correctly applying *Clapper* for speculation, the court interpreted *Clapper* to completely reject the increased risk theory in data breach cases.[241] The court discounted pre-*Clapper* sister circuit court precedent—*Pisciotta*, *Krottner*, and *Ruiz*—as "thinly reasoned."[242] As evidence, it specifically stated that the *Strautins* and *Galaria* courts, among others, "have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases."[243] But, *Strautins* and *Galaria* applied *Clapper* with far too broad of a brush, failing to limit its application to *highly* speculative chains of events and government action.[244]

D. Not so Fast, Clapper

Other courts read *Clapper* for what it really was. Notably, on January 21, 2014, the Southern District of California in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*[245] found standing after a large-scale criminal intrusion into Sony's online gaming network.[246] The network contained customers' names, email and mailing addresses, birth dates, credit and debit card information—including security codes, full numbers, and expiration dates—and login information.[247] Being in the Ninth Circuit, the court considered *Clapper*'s effect on standing and, most importantly, *Krottner*'s viability.

---

likely than not, did not steal the tapes for their contents).

241. *See id.* at 25 ("That increased risk, they maintain, in and of itself confers standing. But as Clapper makes clear, that is not true. The degree by which the risk of harm has increased is irrelevant—instead, the question is whether the harm is certainly impending.").

242. *Id.* at 28. Without providing a reason, the court merely cited *Pisciotta*, *Ruiz*, *Krottner*, and *Century Delta* in passing, treating their reasoning as per se incorrect in light of *Clapper*. *Id.*

243. *Id.* (internal citation omitted).

244. *See supra* notes 201–230 and accompanying text (discussing how these courts have misinterpreted *Clapper* to overrule prior data breach precedent where the hackers had immediate access to the plaintiffs' PII—i.e., the only step left was for the hacker to use the PII to the detriment of the plaintiffs).

245. 996 F. Supp. 2d 942 (S.D. Cal. 2014).

246. *See id.* at 955 (conceding that millions of users' PII was stolen).

247. *Id.* at 954.

Defendants argued that *Clapper* tightened *Krottner*'s injury-in-fact analysis.[248] The court did not agree. It found no reason to interpret *Clapper* as altering, let alone tightening, constitutional standing requirements.[249] By using the term "certainly impending" instead of "real and immediate," the court opined that the Supreme Court did not establish a new standing framework.[250] The court found that motions to dismiss were routinely denied where the plaintiff alleges the collection and wrongful disclosure of PII.[251] Most importantly, the court found that *Krottner* and *Clapper* only require that plaintiffs "plausibly allege[] a credible threat of impending harm based on the disclosure of their Personal Information following the intrusion" to survive a motion to dismiss.[252] Actual access to the plaintiffs' personal information need not be alleged.[253]

"*Clapper* did not change the law governing Article III standing," said the Northern District of California later that same year.[254] On September 4, 2014, the court in *In re Adobe*

---

248. *See* Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010) (finding that plaintiffs needed "a credible threat of harm" that was "both real and immediate, not conjectural or hypothetical" to satisfy standing for future harms).

249. *See In re* Sony Gaming Networks & Customer Data Sec. Breach Lit., 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014) (finding that the Supreme Court merely reiterated traditional standing requirements elicited in *Whitmore*).

250. *See id.* (interpreting the "certainly impending" and the "real and immediate" standards as one in the same because the Supreme Court merely applied long established standing requirements); *see also* Whitmore v. Arkansas, 495 U.S. 149, 160 (1990) (referring to "real and immediate" and "certainly impending" within the same analysis).

251. *See Sony Gaming Networks*, 996 F. Supp. 2d at 961; *see also, e.g.*, *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 711–12 (N.D. Cal. 2011) (finding standing—through a statutory violation—where defendants transmitted to advertisers the identities and the URL of the webpage being viewed when plaintiffs clicked an the advertisement); Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010) (finding standing because there was a real and immediate threat that the plaintiffs' private information would continue to be disclosed).

252. *Id.* at 962.

253. *See id.* (finding that neither *Krottner* nor *Clapper* require plaintiffs to allege actual access to their personal information, and that only a credible threat of impending harm was required to find standing).

254. *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1213 (N.D. Cal. 2014).

Systems Privacy Litigation[255] found standing and reaffirmed *Krottner*'s viability in light of *Clapper*.[256] As in the Sony data breach, the Adobe network contained customers' email addresses, credit card information, bill addresses, names, telephone numbers, etc.[257] The breach here was exactly the type of "sophisticated, intentional and malicious" intrusion that compelled the *Pisciotta* court to find an imminent harm of future injury.[258] The hackers spent several weeks in the database without detection, decrypting and removing over 38 million customers' PII.[259] The plaintiffs alleged three cognizable injuries: "(1) increased risk of future harm; (2) costs to mitigate the risk of future harm; and/or (3) loss of the value of their Adobe products."[260]

Adobe was the first court to recognize *Clapper*'s sensitive constitutional context.[261] It emphasized that *Clapper* merely overruled the Second Circuit's "objectively reasonable likelihood" standard as too broad.[262] It also recognized that the plaintiffs in *Clapper* could only speculate whether the governmental actors would even make the decision to intercept their communications.[263] Finally, it highlighted the Supreme Court's recognition of two separate and distinct standing inquiries; most importantly, the "substantial risk" standard.[264] Given *Clapper*'s

---

255. *Id.*

256. *See id.* at 1214 (finding that *Clapper* and *Krottner* were not irreconcilable).

257. *Id.* at 1206.

258. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007) (focusing on the nature of the cyber attack).

259. *Adobe*, 66 F. Supp. 3d at 1206.

260. *Id.* at 1211.

261. *See id.* (emphasizing that the sensitive constitutional context in *Clapper* called for an "unusually rigorous" standing inquiry (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013))).

262. *See id.* at 1214 ("*Clapper* merely held that the Second Circuit had strayed from these well-established standing principles by accepting a too-speculative theory of future injury.").

263. *See id.* at 1213 (noting that, in *Clapper*, the government would have to decide to target plaintiffs' client's communications, choose to invoke their authority under the particular challenged statute, *and* have an Article III judge decide the constitutionality of the surveillance before any action was taken).

264. *See id.* (referring to footnote 5 of *Clapper* in which the Court recognized the existence of the "substantial risk" standard (citing Clapper v. Amnesty Int'l

limited scope, the court found *Krottner* and *Clapper* reconcilable.[265] The court placed little emphasis on *Krottner*'s alternative language, finding *Krottner*'s phrasing more similar to *Clapper*'s "certainly impending" than to the Second Circuit's "objectively reasonably likelihood."[266] As such, the court found standing under *Krottner*.[267]

Interestingly, the court not only reaffirmed *Krottner*'s viability, but it also found standing under *Clapper* as well.[268] In its opinion, the plaintiffs' risk of their PII being misused was "immediate and very real."[269] The court focused on the fact that the hackers deliberately targeted Adobe's servers, spent several weeks collecting customer PII, and that the plaintiffs' PII was in fact taken during the breach.[270] There was no speculation whether the information was taken.[271] In the courts eyes, the injury could only be more imminent if their PII had already been misused.[272] The court did not believe that plaintiffs should have to "wait until they actually suffer identity theft . . . to establish

---

USA, 133 S. Ct. 1138, 1150 n.5 (2013))). The court interpreted the substantial risk standard to permit plaintiffs to reasonably incur mitigation costs if there is a substantial risk of harm. *Id.* at 1213.

265. *See id.* at 1214 (finding that lower courts in the Ninth Circuit have a duty to reconcile "intervening higher authority" with Ninth Circuit precedent unless higher authority clearly overrules it).

266. *Compare* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) ("[I]mmediate danger of sustaining some direct injury . . . . [C]redible threat of real and immediate harm . . . ."), *with* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) ("[C]ertainly impending . . . ."). Importantly, the court failed to notice that *Krottner*'s "real and immediate" threat test came from the very case that established the certainly impending requirement. *See* Whitmore v. Arkansas, 495 U.S. 149, 160 (1990) ("[T]here is no amount of evidence that potentially could establish that Whitmore's asserted future injury is 'real and immediate.'" (quoting O'Shea v. Littleton, 414 U.S. 488, 494 (1974))). This further supports that *Krottner*'s standard not only is viable, but that it also works hand in hand with the certainly impending standard.

267. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1211–12 (N.D. Cal. 2014) ("Adobe does not dispute that *Krottner* is directly on point.").

268. *See id.* at 1214 ("[E]ven if *Krottner* is no longer good law, the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*.").

269. *Id.* at 1215.

270. *See id.* (expressing the same concern seen in the *Pisciotta* court with regard to the nature of the cyber attack).

271. *See id.* (recognizing that Adobe notified its customers that their *particular* PII was accessed).

272. *Id.*

standing."[273] The Seventh Circuit found this reasoning persuasive.[274]

IV. The Seventh Circuit Answers the Call

As we have seen, even with similar facts, the circuit courts addressed the imminent injury issue extremely differently.[275] After *Clapper*—a non-data breach case—several district courts determined that *Clapper* not only overruled circuit court data breach precedent,[276] but that it tightened the imminent injury standard altogether.[277] Then came *Remijas v. Neiman Marcus Group, LLC*[278] on July 20, 2015, boldly stating: "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing."[279] This makes the Seventh Circuit the first

---

273. *See id.* (refusing to wait for an actual injury because it would run contrary to the established principle that harm need not be "literally certain" (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013))).

274. *See infra* Part IV (discussing the *Remijas* court's application of *Adobe*'s reasoning).

275. *See supra* Part III.A (comparing the differences in circuit courts' treatment of data breach claims).

276. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (increased risk of future harm); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (credible threat of real and immediate injury).

277. *See, e.g.*, Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("*Clapper* compels rejection of Strautins' claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d. 646 (S.D. Ohio 2014) (holding that the increased risk of future harm relying on the occurrence of future criminal actions by independent decision-makers was not imminent or certainly impending); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Cal. Mar. 3, 2013) ("The Complaint alleges Plaintiffs incurred expenses to mitigate an increased risk of identity theft or fraud, but it does not allege what those expenses are with any specificity. *Even if specific expenses had been alleged*, such expenses would not qualify as actual injuries under *Clapper*." (emphasis added)).

278. *See Seventh Circuit Denies En Banc Review For Data Breach Class Action*, HUNTON & WILLIAMS PRIV. BLOG (Sept. 29, 2015), https://www.huntonprivacyblog.com/2015/09/29/seventh-circuit-denies-en-banc-review-for-data-breach-class-action/ (last visited May 12, 2016) (discussing the denial of en banc review for *Remijas*) (on file with the Washington and Lee Law Review).

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

post-*Clapper* circuit court to consider imminent injury in the data breach context.[280]

In *Remijas*, Neiman Marcus sent letters to its customers disclosing that a data breach exposed potentially 350,000 customer credit cards.[281] Importantly, Neiman Marcus offered *all* 350,000 customers credit monitoring and identity-theft protection.[282] The plaintiffs alleged two imminent injuries: "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[283] The court found that those plaintiffs claiming actual identity theft alleged a cognizable injury-in-fact.[284]

"At this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach."[285] Importantly, the court distinguished the case from *Clapper* because here, Neiman Marcus confirmed the breach,[286] whereas in *Clapper*, the plaintiffs only suspected that

---

280. Its decision caused a ripple effect in the district courts. *See* Antman v. Uber Techs., Inc., No. 3:15-CV-01175-LB, 2015 WL 6123054, at *10 (N.D. Cal. Oct. 19, 2015) (citing *Remijas* and *Adobe* in confirming the continuing viability of *Krottner*'s "credible, real, and immediate" future injury test). The court applied *Adobe* and *Remijas'* reasoning to limit *Clapper*. *Id.*; *see also In re* SuperValu, Inc., 2016 U.S. Dist. LEXIS 2592, *15 (D. Minn. Jan. 7, 2016) (distinguishing *Remijas* and *Adobe*, arguing that they apply only where there is clear access and misuse to the PII); Whalen v. Michael Stores Inc., No. 14-CV-7006 (JS)(ARL), 2015 WL 9462108, at *5 (E.D.N.Y. Dec. 28, 2015) ("But one critical distinction in [*Remijas*] is that 9,200 of those customers experienced fraudulent charges following the breach."); Conrad v. Boiron, Inc., 2015 U.S. Dist. LEXIS 152981 ("There must be at least a substantial risk of future harm to the named plaintiff." (citing *Remijas*, 794 F.3d at 693));

281. *See Remijas*, 794 F.3d at 690 (noting that "9,200 of those 350,000 exposed credit cards" were already used fraudulently).

282. *Id.* Ironically, offering this protection hurt the defendant's case because the court reasoned that they would not have provided credit monitoring if the risk was "so ephemeral that it [could] safely be disregarded." *Id.* at 694.

283. *Id.* at 692.

284. *See id.* (conferring standing even though those plaintiffs actually injured had been reimbursed, finding that with identity theft comes lost time and additional expenses to pursue relief and "sort things out").

285. *Id.* at 693 (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) (acknowledging the "substantial risk of harm" standard and implying that it is a lesser standard than "certainly impending").

286. *See id.* at 694 ("Neiman Marcus does not contest the fact that the initial breach took place.").

their communications would be intercepted.[287] In *Remijas*, there was no doubt that the information was stolen and its contents were clear.[288] As such, the court found that future injury was imminent.[289] Second, with regard to traceability, it acknowledged an issue particularly relevant to any data breach plaintiff's claim of future harm;[290] the longer a plaintiff "wait[s] for the threatened harm to materialize," the stronger a defendant's traceability defense becomes.[291] Nor did defendant's argument—that any alleged future injuries may arise from other breaches—convince the court that the claim was not fairly traceable to Neiman Marcus.[292]

Third, the court acknowledged the obvious reality inherent in any targeted data breach.[293] All along, courts should have been asking the question—as the *Remijas* court wisely did—"Why else would hackers break into a store's database and steal consumers' private information . . . . [If not] to [eventually] make fraudulent

---

287. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148 (2013) ("[R]espondents' theory necessarily rests on their assertion that the Government will target *other individuals*—namely, their foreign contacts. Yet respondents have no actual knowledge of the Government's §1881a targeting practices." (emphasis added)).

288. *See* Remijas v. Neiman Marcus Grp., LLC., 794 F.3d 688, 693 (7th Cir. 2015) (conceding that 350,000 credit cards were potentially exposed).

289. The nature of the attack, the access to PII, and the free credit monitoring all persuaded the court that there was a substantial risk of future harm and that the mitigation costs were, therefore, in response to an imminent harm. *Id.* at 694.

290. Recall that an injury must "be fairly traceable to the challenged action of the defendant." Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

291. *See Remijas*, 794 F.3d at 693 (citing *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d. 1197, 1215 n.5 (N.D. Cal. 2014)). This directly challenges *Reilly*'s theory that victims of data breach should sue once the injury materializes. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011) ("In a data breach case . . . there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely—if the hacked information is actually read, copied, understood, and misused to a plaintiff's detriment.").

292. *See Remijas*, 794 F.3d at 696 (likening the defendant's argument to that of *Summers v. Tice*, in which the court shifted the burden upon the defendants prove who was responsible (citing Summers v. Tice, 33 Cal. 2d 80, 88 (1944))).

293. As compared to what appeared to be a typical car burglary in *SAIC*. *See supra* notes 231–244 (discussing the *SAIC* court's correct application of *Clapper*).

charges or assume those consumers' identity[?]"[294]Guided by the obvious answer, the court found the plaintiffs' substantial risk of harm plausible.[295]

Finally, with regard to mitigation costs incurred, the court's answer once again appears to follow common sense. The court reasoned that, once a consumer hears that her credit card was stolen, purchasing credit protection is not an unreasonable response.[296] Also, the price of credit protection, such as Experian, is around $19.95 per month after the first month; a cost the court calls "more than *de minimis*."[297] The court found that mitigation expenses were a valid actual injury in response to the substantial risk of harm.[298]

V. In Light of Remijas*, Courts Should Confer Standing for Victims of Targeted Data Breaches*

This Note does not argue that any loss of data creates an imminent injury. Rather, it only argues that *Clapper* did not change preexisting standing requirements and that it has been incorrectly interpreted to deny standing for otherwise legitimate claims. *Clapper* left the circuit court data breach opinions—*Pisciotta* and *Krottner*—intact because they permit an allowable level of speculation inherent in any imminent injury claim. To determine *Clapper*'s proper application, we must consider the level of speculation involved;[299] the circumstances surrounding a

---

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

295. *See id.* (referring to additional government data showing that hackers may wait up to a year before using the information illegally or that the information may be sold or posted on the Internet, leaving open the possibility that fraudulent use of the information could last for years).

296. Especially in light of the fact that Neiman Marcus offered to provide free credit protection to *anyone* who shopped in their stores in between January 2013 and January 2014. *Id.* at 694.

297. *Id.*

298. *See id.* (analogizing to the First Circuit in *Anderson v. Hannaford Bros. Co.*, in which the court found standing where the "plaintiffs sufficiently alleged mitigation expenses—namely, the fees for replacement cards and monitoring expenses . . . [even though] the harm [was] not physical").

299. *See infra* Part V.B (discussing the speculation inherent in all imminent injury claims and limiting *Clapper*'s application to true speculation).

data breach;[300] and the applicable standing inquiry.[301] These elements are critical to *Clapper*'s proper application.

A. The "Certainly Impending" Standard Remains Unchanged

Recall that *Clapper* was a government surveillance case that *reaffirmed* the "well-established requirement that a future injury must be 'certainly impending.'"[302] In reality, the import of the Court's decision is very narrow. First, the Court found the Second Circuit's loose and "novel" "objectively reasonable likelihood" standard inconsistent with the certainly impending standard."[303] It did not purport to heighten the standing inquiry nor did it discard the substantial risk standard.[304] Second, it found that plaintiffs cannot establish standing based on costs incurred mitigating highly speculative future harm—i.e. "manufactur[ing] standing."[305] Third, it reaffirmed that heightened judicial scrutiny applies where courts are forced to speculate into the hypothetical actions of independent government actors.[306]

1. Clapper *is a Scalpel, Not a Wrecking Ball*

The proposition that, "under *Clapper*, more is required to show an injury is certainly impending"[307] is patently incorrect.[308]

---

300. *See infra* Part V.A (distinguishing between malicious targeted cyber attacks directed towards data servers and coincidental data thefts).

301. *See infra* Part V.C (discussing whether to apply the "certainly impending" or "substantial risk" standards in determining imminence).

302. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

303. *See id.* (invalidating the Second Circuit's "novel view of standing").

304. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("[*Clapper*] did not jettison the 'substantial risk' standard." (internal citation omitted)); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1213 (N.D. Cal. 2014) ("The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability.").

305. *See Clapper*, 133 S. Ct. at 1143 (finding that incurring mitigation costs based on a non-imminent harm would permit plaintiffs to essentially purchase their way into court).

306. *Id.* at 1141.

307. *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 656 (S.D. Ohio 2014) (interpreting *Clapper* as heightening standing altogether).

In *Clapper*, the Court did not heighten the certainly impending standard; it was simply not met.[309] The alleged harm failed to satisfy even the less stringent substantial risk standard.[310] If it could not satisfy this lesser standard, it follows that the certainly impending inquiry would fail as well—let alone an allegedly heightened standard.[311] Therefore, there would be no reason for the Court to raise the standard if the baseline was not even satisfied. It logically follows that the standard was not raised; rather, it simply was not met because of the high degree of speculation.[312] Therefore, if the certainly impending standard *has* been heightened, its application must be limited to future harm contingent on speculative decisions of independent government actors.[313]

Furthermore, *Clapper* was not a data breach case. The Court neither discussed data breach case law nor did it question *Krottner*'s standard.[314] *Clapper* merely concluded that the Second Circuit's "objectively reasonably likelihood" standard deviated

---

308. *Clapper* could not have purported to heighten the standard because the chain of events did not even satisfy the substantial risk standard. It was truly speculative regardless of the standard applied.

309. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013) (finding the plaintiffs argument *too* speculative).

310. *See id.* at 1150 n.5 ("But to the extent that the 'substantial risk' standard is relevant and is distinct from the 'certainly impending' requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here.").

311. *See id.* (implying that the substantial risk of future harm standard is less demanding than the certainly impending standard).

312. The speculation coupled with the Court's separation-of-powers concern left the plaintiffs' case doomed from the start. *See id.* at 1144–45 (recognizing that the plaintiffs' case presented a constitutional challenge to a government surveillance statute "subject to congressional oversight and several types of Executive Branch review").

313. In this scenario, prior circuit court precedent must co-exist with *Clapper*. *See, e.g.*, Miller v. Gammie, 335 F.3d 889, 900 (9th Cir. 2003) ("We hold that the issues decided by the higher court need not be identical in order to be controlling. Rather, the relevant court of last resort must have undercut the theory or reasoning underlying the prior circuit precedent in such a way that the cases are clearly irreconcilable.").

314. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010) (finding standing because the court found that the plaintiffs were in "immediate danger of sustaining some direct injury," alleging a "credible threat of real and immediate harm").

from traditional standing law.[315] Regardless, *Krottner*'s standard is more closely worded to *Clapper*'s "certainly impending" standard than the "objectively reasonable likelihood" standard.[316] As the *Adobe* court found, this similarity, coupled with *Clapper*'s lack of intent to alter standing law, reaffirmed *Krottner*'s viability.[317]

2. Speculation and Third-Party Action

Clapper reaffirms the established principle that too much speculation sounds the death knell for any imminence claim.[318] *Clapper* does *not* stand for the proposition that *any* speculation effectively topples a certainly impending imminent injury claim.[319] Once a hacker has unfettered access to PII, a future injury is not highly speculative; injury is the final step.[320] Speculation is inherent in any theory of imminent injury.[321] The

---

315. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013) (finding the Second Circuit's imminence standard too loose to satisfy the traditional certainly impending standard).

316. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (determining that a slight change in *Krottner*'s word usage did not create a test separate and distinct from *Clapper*'s certainly impending standard). This is likely because "real and immediate" and "certainly impending" both came from the same case. Whitmore v. Arkansas, 495 U.S. 149, 154–60 (1990).

317. *See id.* (considering *Krottner*'s different word usage as insubstantial, arguing that its standard was more in line with *Clapper*).

318. *See Whitmore*, 495 U.S. at 157 (acknowledging that imminent injury cases require certain at least some speculation).

319. Or for that matter, a claim relying on a substantial risk of future harm.

320. *See Adobe*, 66 F. Supp. 3d at 1215 ("[T]he threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused."). *But see* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 650 (S.D. Ohio 2014) (discrediting the plaintiffs imminence theory as speculative in light of *Clapper* even after hackers accessed the plaintiffs data).

321. This is not a novel position and is readily accepted in non-data breach case law. For example, in cases involving exposure to toxic substances, there is speculation whether the harm will materialize and to what degree. *See* Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2d Cir. 2006) (noting, in dicta, that exposure to toxic substances could establish a risk of future harm sufficient to constitute an injury-in-fact). In medical malpractice suits, the harm has either already occurred or it is imminent. While a botched procedure may statistically lead to problems in the future, it is never certain until it materializes. *See*

Clapper Court expressly stated that future harm is not required to be "literally certain."[322] Conversely, this suggests that standing permits a certain degree of speculation.

Concededly, the *Clapper* plaintiffs' alleged future injury was speculative regardless of the standard applied.[323] This is a far cry from the common scenario where the *only* remaining step is to use a consumer's PII fraudulently.[324] Speculation is minimal where hackers have unfettered access to stolen PII, especially after a sophisticated attack.[325] The *Galaria* court, for example, incorrectly considered future harm relying on *any* third-party action as speculative.[326] Citing *Clapper*, the *Galaria* court denied standing because the plaintiffs' theory relied on "the actions of independent decision makers."[327] *Clapper*'s import, with regard to independent actors, is far more limited.[328] The *Clapper* Court applied this reasoning to the *government* context because of the

---

Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005) (finding that a defective medical implant creates a increased risk of future harm sufficient to establish a cognizable injury).

322. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) (implying that both the certainly impending and the substantial risk of future harm standards allow for certain degrees of speculation).

323. Recall that the plaintiffs' clients would need to be selected for targeting, they would need to be targeted under the particular statute in question, the Foreign International Surveillance Court would need to authorize the surveillance, and the surveillance would need to be successful. *Clapper*, 133 S. Ct. at 1148.

324. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (recognizing that the minimal speculation required once the data is stolen).

325. *See infra* Part V.B.1 (discussing the particularly high risk of harm resulting from an organized infiltration of a data network).

326. *See* Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 655 (S.D. Ohio 2014) (interpreting *Clapper* to deny standing where future harm relied on actions by any independent parties, failing to recognize *Clapper*'s rigorous standing inquiry in the context of independent *governmental* decision makers).

327. *See id.* (taking *Clapper*'s emphasis on independent decision makers out of context (citing *Clapper*, 133 S. Ct. at 1141))). According to the court, any alleged injury is "contingent on what, if anything . . . third party criminals do with th[e] information." *Id.*

328. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144–45 (2013) (noting that § 1881a was subject to congressional and Executive Branch review, and subject to Fourth Amendment limitations where independent judges determined the constitutionality of any proposed foreign surveillance).

separation-of-powers concern.[329] It was not intended to foreclose *any* future harm contingent on the actions of non-governmental third parties.[330]

B. The Nature of Data Breach and Ease of Access to Stolen Information

The circumstances surrounding a breach are particularly relevant in determining whether *Clapper* applies and the nature of the speculation involved.[331] As we have seen, one can hardly call a car burglary a "data breach" merely because a data tape happened to be stolen along with other valuable electronic equipment.[332] A targeted attack on a corporation's data server, however, is another story. The theft of a laptop containing unencrypted PII requires its own and different considerations. If the criminal does not intend to steal data but a physical theft results in *unfettered access*, this raises a future injury towards certainly impending.[333] As such, the nature of the breach and the

---

329. When the Court claimed its traditional reluctance to speculate into the actions of independent decision makers, it cited *Whitmore* and *Lujan*, both requiring speculation into the actions of governmental actors. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 561–62 (1992) ("When the suit is one challenging the legality of *government action or inaction* . . . ." (emphasis added)); Whitmore v. Arkansas, 495 U.S. 149, 159–60 (1990) ("It is just not possible for a litigant to prove in advance that *the judicial system* will lead to any particular result in his case." (emphasis added)).

330. *See, e.g.*, United States v. Students Challenging Regulatory Agency Procedures (SCRAP), 412 U.S.669, 678 (1973) (granting standing where plaintiffs alleged that imminent "economic, recreational and aesthetic harm" would result from the Interstate Commerce Commission's approval of a railroad surcharge). The Court further found the alleged harms, even if incorrect, sufficient to survive a motion to dismiss because they *may* be able to show that the "string of occurrences alleged would happen immediately." *Id.* at 159.

331. *See infra* notes 332–358 and accompanying text (arguing that unfettered access to PII, regardless of the thief's intent, creates a sufficiently imminent injury).

332. *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) ("The tapes could be uploaded onto her computer and fully deciphered, or they could be lying in a landfill somewhere in Texas because she trashed them after achieving her main goal of boosting the car stereo and GPS.").

333. *See, e.g.*, Riley, *supra* note 12 (noting that credit card information can be sold on the internet for around $3.50 per number). Note that, even if the thief does not have access to the "deep web" market for credit card numbers, he has

ease of access to PII are particularly relevant considerations when determining imminence.[334]

1. The Sophisticated Attack

Some cases conferring standing emphasized the hackers' specific targeting methods and sophistication when determining imminence.[335] The *Pisciotta* court emphasized the breach's "sophisticated, intentional and malicious" nature;[336] *Adobe* and *Remijas* followed suit.[337] Recognizing the sophisticated and calculated nature of a breach is critical to whether an injury is imminent, but some courts ignore it altogether.[338] Rather, they deny standing even where a defendant concedes that hackers

---

all the information necessary to make fraudulent charges. *See* Pierluigi Paganini, *Buying Personal Information in the Deep Web*, INFOSEC INST. (Mar. 24, 2015), http://resources.infosecinstitute.com/buying-personal-information-in-the-deep-web/ (last visited May 12, 2016) ("The term underground ecosystem is usually used to refer a collection of forums, websites and chat rooms that are designed with the specific intent to advantage, streamline and industrialize criminal activities.") (on file with the Washington and Lee Law Review).

334. *See infra* Parts V.B.1–2 (differentiating between sophisticated cyber attacks and physical theft of electronics containing PII, but ultimately concluding that both instances present an imminent injury where nothing more is required to access the data).

335. *Compare* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631–32 (7th Cir. 2007) (granting standing after a sophisticated and malicious attack on a data server without considering whether or not the hackers copied or disseminated the data), *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1206 (N.D. Cal. 2014) (granting standing after hackers breached *Adobe*'s data network, spent weeks inside, and removed customer data, all without detection), *and* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (granting standing where hackers potentially gained access to 350,000 consumers' credit card information), *with* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (granting standing after a laptop containing the unencrypted PII of thousands of employees was stolen), *and* Ruiz v. Gap, 380 F. App'x 689, 690 (9th Cir. 2010) (granting standing after a laptop containing 750,000 unencrypted employment applications was stolen).

336. *Pisciotta*, 499 F.3d at 632.

337. *See Adobe*, 66 F. Supp. 3d at 1214 ([T]he hackers deliberately targeted Adobe's servers and spent several weeks collecting names . . . ."); *Remijas*, 794 F.3d at 693 ("[T]he hackers deliberately targeted Neiman Marcus in order to obtain their credit-card information . . . .").

338. *See supra* Parts III.A,C (arguing that *Clapper* has blinded the courts to the obvious imminence of future harm after a sophisticated cyber attack).

possess the plaintiffs PII after a cyber attack.[339] Other courts concede that hackers infiltrated a data system, but refused to recognize they could have actually saved or read customer PII.[340]

Hackers, by virtue of their "profession," possess a specific set of skills unknown to the layperson.[341] Hacking into a data network, presumably, is done for a specific purpose—to access the data behind the encryption software.[342] Once this data is accessed and seen by unauthorized eyes, the damage is done—the hackers have all the information necessary to harm the plaintiffs.[343] The *Adobe* court found that once data is accessed, the only step left for a harm to occur is the harm itself.[344] Additionally, *Remijas* noted that the longer a plaintiff waits to sue, the harder it is to prove

---

339. *See supra* Parts III.A,C (discussing the *Strautins* and *Galaria* courts' lack of legitimate consideration of the circumstances surrounding a cyber attack).

340. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) ("An unknown hacker infiltrated Ceridian's Powerpay system and *potentially* gained access to personal and financial information . . . . It is not known whether the hacker read, copied, or understood the data." (emphasis added)).

341. *See The Essential Skills to Becoming a Hacker*, WONDERHOWTO: NULL-BYTE (2015), http://null-byte.wonderhowto.com/how-to/essential-skills-becoming-master-hacker-0154509/ (last visited May 12, 2016) ("As the hacker is among the most skilled information technology disciplines, it requires a wide knowledge of IT technologies and techniques.") (on file with the Washington and Lee Law Review).

342. Given the complex set of skills that hacking requires and the degree of criminal liability involved, hackers capable of breaching a corporate data network presumably do not do so without intending to see the encrypted information. *See 10 Ways Companies Get Hacked*, CNBC (Apr. 14, 2015), http://www.cnbc.com/2012/07/06/10-Ways-Companies-Get-Hacked.html (last visited May 12, 2016) (identifying sophisticated methods that hackers use to gain entry into corporate data networks) (on file with the Washington and Lee Law Review).

343. We have seen various types of damaging PII stolen throughout this discussion. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (credit card information); *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (same); *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *4 (N.D. Cal. Mar. 3, 2013) (same); *see also In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (names, addresses, contact information, medical records); *Reilly*, 664 F.3d at 40 (personal and financial information); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d. 646, 650 (S.D. Ohio 2014) (financial information, including social security numbers).

344. *Adobe*, 66 F. Supp. 3d at 1215 (conferring standing even though any identity theft relied on actions by third parties).

traceability.[345] In its justification, the *Remijas* court pointed to evidence showing that victims of data breach remain exposed for many years.[346] This could lead to identity theft long after free credit monitoring expires, leaving plaintiffs without a remedy in court.[347] In this light, the conclusion that harm is speculative after a sophisticated and intentional data breach appears bizarre to say the least. Yet, some courts interpret *Clapper* to require such a result.[348]

2. The Average Thief's Windfall

A burglar breaks into a house and among the items he steals is what appears to be an ordinary laptop. But what happens when the laptop contains the unencrypted credit card numbers and personal information of tens of thousands of people? Admittedly, future harm from theft of an encrypted laptop or data tape requires highly speculative steps.[349] Unlike a sophisticated cyber attack, the average thief does not have the skills to decrypt a laptop or read—or even recognize the significance of—a data tape.[350] However, on a decrypted laptop, a hacker's ease of access to the data is readily apparent, and the

---

345. *Remijas*, 794 F.3d at 693 (bolstering its traceability analysis with the fact that Neiman Marcus already raised it as a defense).

346. *See id.* at 694 ("[S]tolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.").

347. *See id.* (noting that plaintiffs are left vulnerable to attack for several years and that it becomes increasingly difficult to trace any damages to the defendant, especially given the increasing frequency of data breaches).

348. *See supra* Part III.C (discussing cases that denied standing where hackers gained access to the particular plaintiffs PII after a sophisticated breach).

349. Certain levels of speculation are inherent and permitted in any imminence claim. *See supra* note 330 (discussing *SCRAP*—a case cited by *Whitmore* when it established the certainly impending standard—where the court granted standing because the plaintiffs could possibly prove the immediacy of the alleged injury during trial).

350. *See In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (denying standing based on the speculative chain of events required to actually read the information on the stolen data tapes).

harm is real and immediate.[351] As we have seen, with successful and deliberate targeting comes ease of access to data and the only remaining step is injury.[352] This same immediacy is present were thief has the valuable PII at his fingertips.[353] There is no speculation whether he will recognize the information for what it is or that special means must be used to access it.[354]

C. Reconciling Competing Circuit Standards in Light of a Limited Clapper

With *Clapper* properly limited, data breach victims can establish standing under two theories: (1) the certainly impending or (2) the substantial risk standards.[355] In this discussion, many theories for standing have come to light from different circuits.[356] *Pisciotta* was the first circuit to tackle the issue.[357] Analogizing to toxic tort, medical malpractice, and environmental cases, the court found that an increased risk of

---

351. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Here, Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."); Ruiz v. Gap, 380 F. App'x 689, 691 (9th Cir. 2010) (granting standing under *Century Delta*'s "credible threat of harm" standard (citing Cent. Delta Agency Water Agency, 306 F.3d 938, 950 (9th Cir. 2002))); Enslin v. Coca-Cola Co., No. 2:14-CV-06476, 2015 WL 5729241, at *14 (E.D. Pa. Sept. 30, 2015) (granting standing where plaintiffs suffered *actual* injuries stemming from laptop theft).

352. The *Sony*, *Adobe* and *Remijas* courts do not ignore the obvious implications of a sophisticated data breach. *See supra* notes 245–298 (conferring standing where data was accessed after a sophisticated breach).

353. *See Krottner*, 628 F.3d at 1143 (conferring standing where a thief had unfettered access to PII).

354. Note in *SAIC*, the court denied standing because to the average person, data tapes are not readily recognizable. *SAIC*, 45 F. Supp. 3d at 25. This is clearly distinguishable from an unencrypted list of PII.

355. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (finding that the plaintiffs satisfied both *Krottner* and the certainly impending standard);

356. *See supra* Part III (discussing the standards applied in *Clapper*, *Pisciotta*, and *Krottner*, and how courts have interpreted them).

357. *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (citing to sister circuit courts in an attempt to analogize toxic tort, medical malpractice, and environmental harm cases to data breach lawsuits).

harm was sufficient to confer standing.[358] As noted, speculation is inherent in any imminent injury claim.[359] We have seen that *Clapper*, properly limited, only forecloses standing theories relying on a "highly speculative" and "highly attenuated" chain of events.[360] Therefore, where PII is readily accessible to hackers or identity thieves, the only step remaining is for the harm to occur.[361] It follows that, even if *Pisciotta*'s standard *is* more similar to an "objectively reasonable likelihood," a substantial risk of harm still existed and, most likely, the harm was certainly impending.[362]

Krottner, following *Pisciotta*, found standing where the plaintiffs faced "a credible threat of harm that was both real and immediate, not conjectural or hypothetical."[363] *Krottner* reached this conclusion through similar analogies to other non-data breach cases cited in *Pisciotta*.[364] The standard, however, is more akin to the traditional "certainly impending standard."[365] *Krottner*, while reiterating that an imminent harm exists, set the appropriate standard slightly above *Pisciotta*. This was not a mere increased risk of harm, rather, the harm was "real and immediate."[366]

---

358. For cases discussing personal injury, see Denney v. Deutsche Bank AG, 443 F.3d 253 (2d Cir. 2006); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568 (6th Cir. 2005). For cases discussing environmental harm, see Cent. Delta Water Agency v. United States, 306 F.3d 938 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000).

359. *See supra* Part V.A.2 (discussing allowable levels of speculation in imminence claims).

360. *See supra* Part V.A.2 (conceding that *Clapper* was rightfully decided given the speculative nature of plaintiffs alleged future injuries).

361. *See supra* Part V.A.2 (noting that *Clapper* only rejects imminence theories that require speculation into the actions of independent *governmental* actors).

362. As seen in *Adobe*—which was decided on similar facts—the court found that the plaintiffs satisfied the certainly impending requirement. *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014).

363. Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (internal citations omitted).

364. *See* cases cited *supra* note 330 (listing toxic tort, medical malpractice, and environmental cases all granting standing for an increased risk of future harm).

365. *See supra* notes 305–307 (likening *Krottner*'s standard to be more similar to "certainly impending" than an "objectively reasonable likelihood").

366. The court noted that, had the plaintiffs alleged future harm from a

As an aside, it is important to address *Reilly*'s criticism of *Pisciotta* and *Krottner*'s analogy to toxic tort, medical malpractice, and environmental cases.[367] *Reilly* appears to stand for the proposition that, if future identity theft can only be articulated using the word "if," it is not imminent.[368] But such a reading leaves no effective method of redressing harms stemming from data breaches. The court found that, as opposed to someone's health or the destruction of a wilderness habitat, the only thing at stake was money.[369] Because monetary damages are quantifiable at the time of the actual harm, the court argued that suit should be brought once the injury occurs.[370] Given that injury can occur over one year after a breach[371] coupled with the high frequency of data breaches,[372] it would be increasingly difficult to prove traceability.[373]

The *Adobe* court found that harm is certainly impending where hackers have access to PII.[374] In fact, the only way an

---

future theft of the laptop, then the threat would be "far less credible." *Krottner*, 628 F.3d at 1143.

367. *See supra* notes 127–135 (discussing *Reilly*'s reliance on the policies surrounding toxic torts, medical malpractice, and environmental suits and how the court found them inapplicable in the data breach context).

368. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) ("[W]e cannot now describe how Appellants will be injured in this case without beginning our explanation with the word 'if' . . . .").

369. *Id.* at 45–46.

370. *See id.* at 45 ("In a data breach case, however, there is no reason to believe that monetary compensation will not return plaintiffs to their original position completely . . . .").

371. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) ("[S]tolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.").

372. *See* Chen, *supra* note 10 (discussing the rise in identity theft, reporting that in 2014, there were over 250,000 successful identity thefts in America alone).

373. *Remijas*, 794 F.3d at 694 (citing *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)). In *Adobe*, the defendant used the very argument that, as time goes on without injury, it is more and more unlikely that any future injury was defendants fault. *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014).

374. *See Adobe*, 66 F. Supp. 3d at 1215 (finding *Clapper* inapplicable because there was no speculation whether the information was stolen); *Remijas*, 794 F.3d at 696 (finding that, once data thieves obtained unencrypted customer data, victims should not have to wait for an actual injury to occur before having

injury could be more imminent was if the data was already misused.[375] To the court, the only speculation to consider was whether the plaintiffs' information had been stolen.[376] The court found that waiting for the injury to occur would run counter to the proposition that future harm need not be "literally certain."[377]

Interestingly, the *Remijas* court used *Adobe*'s "real and immediate harm"—which came from *Krottner*—to satisfy the "substantial risk" standard acknowledged in *Clapper*. The court found that the "deliberate targeting" evidenced an "immediate and very real" threat that was not "highly attenuated" and "highly speculative."[378] The court correctly interpreted *Clapper* only to foreclose high levels of speculation.

The *Pisciotta*, *Adobe*, and *Remijas* interpretations all have one element in common; they find standing where a network was deliberately targeted.[379] They also tend to show that, at minimum, a targeted breach satisfies the "substantial risk" standard.[380] While *Pisciotta*'s reasoning would not likely survive today, its similarity to more recent cases shows that the plaintiff's claim would survive under a substantial risk of harm.[381] *Krottner*'s reasoning, on the other hand, applies to the context where stolen data is readily available regardless of the thief's intent to steal PII.[382] Even without a clear and deliberate targeting of PII, immediate access to data presents a "real and

---

standing to sue—the breach created a "substantial risk" of future identity theft).

375. *See Adobe*, 66 F. Supp. 3d at 1215.

376. *See id.* (comparing the present case to *Clapper* where there was no evidence that the communications had been, or would be, monitored under the specific statute).

377. *See id.* (requiring the plaintiffs to wait for an injury to occur would essentially render any imminent injury standard superfluous (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013))).

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

379. *See* cases cited *supra* note 335 (comparing deliberate and accidental theft cases).

380. *See Remijas*, 794 F.3d at 693 (conferring standing where plausibly pled a substantial risk of future harm).

381. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 (N.D. Cal. 2014) (conferring standing on similar facts).

382. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (applying a slightly reworded version of the certainly impending standard—the standard that many post-*Clapper* use to deny standing in identical situations).

immediate" threat of future harm.[383] Readily accessible PII leaves thieves in the same position as hackers after an intentional attack; in both scenarios, the only "speculation" left is for the injury to occur.[384] In light of a properly limited *Clapper,* that neither overruled the substantial risk standard nor raised the certainly impending standard, data breach plaintiffs have an imminent harm sufficient to confer standing.

VI. Conclusion

Remijas, as the first circuit to consider imminent injury in data breach after *Clapper*, legitimately reopens the door for victims. *Clapper* shows no signs of heightening the certainly impending requirement. It absolutely does not call for toppling imminent injury claims when the only "speculative" act is the harm itself. Furthermore, *Clapper* was neither a data breach case nor did it consider the circuit precedent for standing in data breach case law. It merely applied the certainly impending standard and found that it was not satisfied. This outcome was proper given the highly attenuated and highly speculative chain of events.

Clapper stands to maintain the traditional certainly impending standing requirement at its proper level—a highly speculative chain of events effectively defeating a claim of imminent injury. Likewise, it reaffirmed the legitimate judicial wariness involved when a theory of future harm speculates into the actions of independent governmental actors. The Court's heightened scrutiny exemplified this caution, noting its reluctance to pass judgment on speculative future actions of the two other government branches.

In this light, *Remijas* took *Clapper* for exactly what it was. It was not a bar to imminent injury claims flowing from data breaches. In fact, it does not apply at all. Injury is imminent when a thief has access to PII, whether acquiring it was intentional or not. A victim should not have to wait until the injury occurs. Given the minimal speculation involved, the

383. *See Adobe*, 66 F. Supp. 3d at 1215 (finding *Krottner*'s "real and immediate" very similar to "certainly impending").

384. *Id.*

presence of a ready market for PII, and the ease of credit card fraud, there is a substantial risk for future harm (if the harm is not certainly impending). *Clapper* neither forecloses this conclusion nor should it be interpreted to do so.