Washington and Lee Journal of Civil Rights and Social Justice

Volume 25 | Issue 1 Article 8

3-11-2019

Bytes Bite: Why Corporate Data Breaches Should Give Standing to Affected Individuals

Caden Hayes
Washington and Lee University School of Law, Hayes.c@law.wlu.edu

Bytes Bite: Why Corporate Data Breaches Should Give Standing to Affected Individuals†

Caden Hayes*

Table of Contents

---

† 2018 Louise A. Halper Award Winner for Best Student Note

* Candidate for J.D., May 2019, Washington and Lee University School of Law.

Introduction

On July 31st, 2017, Mr. Richard Smith, then CEO of Equifax, woke up thinking it would be a normal Monday.[1] He went to work and held a seemingly routine meeting with the company's Chief Information Officer ["CIO"].[2] Unfortunately, this was no routine meeting: The CIO was informing Mr. Smith that an unknown individual accessed the Equifax's databases.[3] However, the CIO believed that the scale of the data breach was quite small, with no personal information being exposed.[4] So, they both concluded that there was no reason to panic.[5] Nevertheless, pursuant to the company's internal protocol, Equifax retained both a law firm and a cybersecurity firm to begin investigating what had occurred and, more importantly, how broad the damage was.[6] For the next several weeks, investigators worked around the clock, rebuilding every command that was issued and finding out exactly what happened.[7] Finally, on August 15th, Mr. Smith's worst fear was realized: Personal information was indeed stolen from the Equifax databases.[8]

The story the investigators pieced together is as follows. In March 2017, the United States Department of Homeland Security

1. Richard F. Smith, Prepared Testimony of Richard F. Smith Before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection 3 (Oct. 3, 2017) (unpublished manuscript) http://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

2. *Id.* at 3.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.* at 4.

8. *Id.*

found a major security vulnerability in a common business server platform called Apache Struts.[9] A letter was sent out to all major businesses that use Apache Struts to make sure a fix was implemented as soon as possible.[10] Equifax got the letter, but, for some unknown reason, did nothing in response.[11] In May, two months after Homeland Security's letter, hackers used this vulnerability to gain access to the Equifax systems, quickly installing a backdoor.[12] This meant that even if Equifax then patched their systems to fix the Apache Struts issue, it was too late, the hackers were in.[13] The hackers then handed the reins over to a more sophisticated hacking group and, for the next few months, the new group rooted around Equifax's systems.[14] By the time the hackers were discovered, they had stolen or otherwise accessed roughly 143 million people's personal information: A third of the United States' population.[15] On September 7th, Equifax announced to the world what had happened.[16] In response, Mr. Smith was compelled to testify before Congress and later resigned as CEO of Equifax.[17]

This was not the first time valuable financial information has been illegally accessed.[18] Three years ago, Yahoo!'s databases were hacked and every one of Yahoo!'s 3,000,000,000 email accounts

---

9. *Id.* at 2–3.

10. *Id.* at 3.

11. *Id.*

12. *Id.*

13. *See* Michael Riley, Jordan Robertson, & Anita Sharp, *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG BUSINESSWEEK (Sept. 29, 2017 9:09 AM), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros (explaining the fact that it was too late to fix the vulnerability in the Equifax system once hacked) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

14. *See id.* ("[A]s the attack escalated over the following months, that first group—known as an entry crew—handed off to a more sophisticated team of hackers.").

15. *Id.*

16. *See* Smith, *supra* note 1, at 5 ("On September 7, 2017, Equifax publicly announced the breach through a nationwide press release.").

17. *Id.* at 1.

18. *See* Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html (last updated Oct. 3, 2017) (explaining the story of the most recent Yahoo! hack and the subsequent history) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

were accessed.[19] The thieves made off with names, birth dates, phone numbers, security question answers, and backup email addresses used to reset lost passwords.[20] While this information seems unimportant, it becomes particularly damaging when taking into account that it could be used to access other, more important systems, such as government computers.[21] Indeed, an Eastern European hacking collective has reportedly sold this information at least three times, and it is unknown what the buyers will do with that data.[22] Unfortunately for everyone, these are only a few of the many examples of hackers compromising systems to illicitly obtain information for financial benefit.[23]

Hackers have also attacked systems to reveal secrets that have significantly less economic value.[24] The largest example of this was the Ashley Madison hack.[25] Ashley Madison is a well-known website that has one purpose: Facilitate affairs between married individuals.[26] Because of its unique goal, privacy is *incredibly* important.[27] Yet, in 2015, a group called "Impact Team" hacked into Ashley Madison's servers and accessed the names, phone numbers, and credit card information of the site's

---

19. *Id.*

20. *Id.*

21. *See id.* (explaining the information obtained would be useful to a hacker trying to access government computers).

22. *See id.* ("[L]ast August, a hacking collective based in Eastern Europe quietly began offering Yahoo's information for sale.")

23. *See, e.g.*, Nick Wells, *How the Yahoo Hack Stacks Up to Previous Data Breaches*, CNBC (Oct. 4, 2017, 12:25 PM), https://www.cnbc.com/2017/10/04/how-the-yahoo-hack-stacks-up-to-previous-data-breaches.html (listing other examples of unauthorized data access and subsequent disclosure by third parties) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

24. *See* Tom Lamont, *Life After the Ashley Madison Affair*, GUARDIAN (Feb. 27, 2016 7:05 PM), https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked (explaining the story of how Ashley Madison was hacked and the subsequent history) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

25. *See id.* ("[H]ackers leaked the names of 30 million people who had used the infidelity website Ashley Madison.").

26. *See id.* (explaining the intention of Ashley Madison to help married people have affairs with each other).

27. *See id.* ("Ashley Madison claimed to have an international membership of 37.6 million, all of them assured that their use of this service would be anonymous, 100% discreet.").

roughly 37 million users.[28] They even had some information on users' height, weight, and erotic preferences.[29] Impact Team then threatened to publicly release this information unless Ashley Madison shut down.[30] Ashley Madison refused, so, on August 18th, Impact Team released the information.[31] The released names included senior executives, priests, celebrities, military members, and the list goes on.[32] Those revealed were publicly shamed and ridiculed.[33] In Alabama, for example, a newspaper printed all the names of those who were using the website and lived in the area.[34] Marriages were destroyed, business executives resigned, and some people even committed suicide.[35]

These high-profile hacks are not uncommon.[36] In fact, according to the Privacy Rights Clearinghouse, there have been at least 7,961 data breaches, exposing over 10,000,000,000 accounts in total, since 2005.[37] These shocking numbers are not particularly surprising when taking into account the value of information stolen.[38] For example, cell phone numbers, as exposed in the

---

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *See id.* ("[P]oliticians, priests, military members, civil servants, celebrities–these and hundreds of other public figures were found among the listed membership.").

33. *See id.* ("Moral crusaders, operating with impunity, began to shame and squeeze the exposed.").

34. *See id.* ("In Alabama editors at a newspaper decided to print in its pages all the names of people from the region who appeared on Ashley Madison's database.").

35. *See id.* (describing the unfortunate aftermath of the information leak).

36. *See* Wells, *supra* note 23 (listing other examples of unauthorized data accesses and subsequent disclosure by third parties).

37. *See Data Breaches*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breaches (last visited Feb. 21, 2018) (listing the number of publicly disclosed data breaches and how many accounts have been exposed from them) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

38. *See* CESAR CERRUDO & ESTEBAN MARTINEZ FAYO, HACKING DATABASES FOR OWNING YOUR DATA 3 (2007), https://www.blackhat.com/presentations/bh-europe-07/Cerrudo/Whitepaper/bh-eu-07-cerrudo-WP-up.pdf (listing the value of various personal information on the black market) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

Yahoo! hack above, are worth $10 a piece on the black market.[39] The Yahoo! hack exposed 3,000,000,000 phone numbers.[40] Taking that number and multiplying it by the value of a cell phone number, $10, the hackers stood to make $30,000,000,000 from that one hack. That dollar amount does not even consider copies the hackers could make and later resell. Yet while these hackers make astronomical payoffs, the release of this information damages people's lives in multiple ways.[41] Some suffer immense emotional turmoil, others are left in financial ruin.[42] Nevertheless, there is a deep circuit split as to whether the fact that information was stolen is intrinsically sufficient to grant standing to those whose information was stolen to sue the hacked entity.[43] In particular,

---

39. *See id.* (listing the value of cell phone numbers on the black market).

40. *See* Nicole Perlroth, *supra* note 18 (listing the number of Yahoo! accounts compromised).

41. *See* Lamont, *supra* note 24 (explaining the damage caused by the Ashley Madison hack); *see also* Riley, Robertson, & Sharp, *supra* note 13 (explaining the damage caused by the Equifax hack).

42. *See* Lamont, *supra* note 24 (explaining the damage caused by the Ashley Madison hack); *see also* Riley, Robertson, & Sharp, *supra* note 13 (explaining the damage caused by the Equifax hack).

43. *Compare* Beck v. McDonald, 848 F.3d 262, 276–77 (4th Cir.) *cert. denied*, 137 S. Ct. 2307 (2017) (finding that the threat of injury was too speculative to grant standing to plaintiffs whose data was illicitly accessed by third parties while in the care of the defending party), *and In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (finding that the threat of injury was too speculative to grant standing to plaintiffs whose data was stolen from defendant); *and* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d. Cir. 2011) (same), *with* Galaria v. Nationwide Mutual Insurance Comp., 663 F. App'x 384, 390–91 (6th Cir. 2016) (finding that there is sufficient injury to grant standing when a plaintiff's information is illegally stolen from the defending party), *and* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 696 (7th Cir. 2015) (finding the injury requirement satisfied when a plaintiff's information is illegally stolen from the defending party because there is a "substantial risk" that future harm will occur (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (internal quotation marks omitted))), *and* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) ("If a plaintiff faces 'a credible threat of harm' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III . . . . On these facts . . . Plaintiffs . . . have sufficiently alleged an injury-in-fact for purposes of Article III standing." (first quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002); and then quoting City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1938))), *and* Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding sufficient injury to grant standing for plaintiffs whose information was hacked from defendant, particularly noting the costs plaintiffs incurred to mitigate future damages).

the question becomes, "is the increased risk of future injury enough to grant standing?"[44] In Part I of this note, I will briefly discuss the history of constitutional standing and the current test. In Part II, I will explain the aforementioned circuit split. In Part III of this note, I will argue why the courts should answer the question above in the affirmative: The increased risk of future injury is sufficient to grant standing. In Part IV, I will argue alternative ways that courts could and should find sufficient injury to grant standing if the significantly increased risk of future injury is not enough. I note at the outset that this note only deals with the question of standing, not necessarily the merits of any case or any other possible defenses, such as sovereign immunity or the economic loss rule.

I. Traditional Standing Requirements

A. History of Standing

The United States Constitution limits courts to only hear "cases" and "controversies."[45] Whether a lawsuit is a case or controversy, as defined above, is the question of standing.[46] That question is a threshold one.[47] It must be resolved before deciding the merits on a case, even if neither party challenges it.[48] Modern constitutional standing first began in the case of *Fairchild v. Hughes*,[49] where the Supreme Court ruled that a plaintiff must have a direct injury to sue.[50] It was later reinforced in

44. *See, e.g.*, *Beck*, 848 F.3d at 276–77 (finding that the *threat of injury was too speculative to grant standing* to plaintiffs whose data was illicitly accessed by third parties while in the care of the defending party (emphasis added)).

45. *See* U.S. CONST. art. III, § 2, cl. 1 ("The judicial Power shall extend to all Cases [and] . . . controversies.").

46. *See* Lujan v. Def. of Wildlife, 504 U.S. 555, 560 (1992) ("[S]etting apart the 'Cases' and 'Controversies' that are of the justiciable sort referred to in Article III . . . is the doctrine of standing." (quoting U.S. CONST. art. III, § 2, cl. 1)).

47. *See* Orr v. Orr, 440 U.S. 268, 271 (1979) (addressing preliminary questions of standing before addressing the merits of the case, even though neither party challenged standing).

48. *See id.* (same).

49. *See* Fairchild v. Hughes, 258 U.S. 126, 129–130 (1922) (ruling that a private citizen cannot challenge the validity of a statute or a constitutional amendment without direct injury).

50. *See id.* at 129 (finding that a private citizen cannot sue to stop a statute

Massachusetts v. Mellon.[51] From there, standing evolved, eventually becoming the modern three part test of *Lujan v. Defenders of Wildlife*.[52]

B. Current Standing Requirement

The current constitutional minimum for standing has three elements:

> First, the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized . . . and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be "fairly . . . trace[able] to the challenged action of the defendant . . . . Third, it must be likely, as opposed to merely speculative, that the injury will be 'redressed by a favorable decision.[53]

The plaintiff must prove each element.[54] Although, "general factual allegations of injury resulting from the defendant's conduct may suffice."[55] If there is no standing, the judicial system cannot hear the case for want of subject-matter jurisdiction.[56]

In *Clapper v. Amnesty Int'l USA*,[57] the U.S. Supreme Court further explained the "injury in fact" requirement for standing.[58]

---

from passing without a direct injury).

51. *See* Massachusetts v. Mellon, 262 U.S. 447, 488 (1923) (finding that the constitution's separation of powers requires the judicial system to only hear cases where an individual has been directly injured).

52. *See* Lujan v. Def. of Wildlife, 504 U.S. 555, 560–61 (1992) (ruling that plaintiffs must be injured, that injury must have been caused by the defendant, and a favorable ruling can redress the injury).

53. *Id.* (internal quotation marks omitted) (internal citations omitted).

54. *See id.* at 561 ("The party invoking federal jurisdiction bears the burden of establishing these elements.").

55. *Id.*

56. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 624 (D.C. Cir. 2017) (concluding that without Article III standing, the judicial system loses subject-matter jurisdiction (citing *Lujan*, 504 U.S. at 560–61)).

57. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013) (holding that the respondents lacked Article III standing because future injury was not imminent).

58. *See id.* at 409 (explaining further how to satisfy the injury-in-fact requirement).

Specifically, the Court said "'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient."[59] Courts subsequently interpreted this to mean that the injury requirement is fulfilled if it is found that there is a substantial risk for future harm to occur, even if it is not a complete certainty.[60]

The Supreme Court further elucidated this requirement in *Spokeo, Inc. v. Robins*.[61] As stated before, the injury (or threat of future injury) must be both particularized and concrete.[62] For an injury to be particularized "[the injury] must affect the plaintiff in a personal and individual way."[63] While particularized is important, it is different from concrete.[64] A concrete injury is an injury that is "real, and not abstract."[65] However, "concrete" is not necessarily synonymous with "tangible."[66] While tangible is easy to recognize as a "concrete" injury, there are intangible, concrete injuries.[67] In determining whether an intangible harm constitutes an injury sufficient for Article III standing, the Court gave three guides.[68] First, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[69] Second, "because Congress is well

---

59. *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

60. *See, e.g.*, Galaria v. Nationwide Mutual Ins. Comp., 663 F. App'x 384, 388 (6th Cir. 2016) ("[T]he Supreme Court has also 'found standing based on a substantial risk that the harm will occur' . . . even where it is not 'literally certain the harms . . . will come about.'") (internal citations omitted).

61. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (explaining the nuances of the injury requirement of constitutional standing).

62. *See id.* ("To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.") (internal citations omitted).

63. *Id.*

64. *See id.* ("Particularization is necessary to establish injury in fact, but it is not sufficient.").

65. *Id.*

66. *Id.* at 1549.

67. *See id.* ("Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

68. *See id.* (presenting the three requirements for an intangible harm to constitute an injury in order to satisfy Article III standing).

69. *Id.*

positioned to identify intangible harms that meet minimum Article III standing requirements, its judgment is also instructive and important."[70] Lastly, common law can also create intangible harms that satisfy the injury requirement of Article III standing.[71]

With this precedent in mind, the Supreme Court created two tests to determine if future injury satisfies the injury-in-fact standing requirement: The "certainly impending" and "substantial risk" tests.[72] The "certainly impending" test requires that the injury does not rely upon a "highly attenuated chain of possibilities" and is imminent.[73] The "substantial risk" test requires a finding that there is a "substantial risk that the harm will occur."[74] If either test is satisfied, there is sufficient injury to satisfy the injury-in-fact requirement of standing.[75]

II. Case Law Examining This Issue

As mentioned above, there is a circuit split on this issue of standing in data breach cases.[76] The Fourth, Eighth, and Third Circuits have each ruled that plaintiffs have no standing to sue an entity when the plaintiff's information was illegally stolen from that entity.[77] Those courts concluded that there had not yet been

---

70. *Id.*

71. *See id.* ("[T]he law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure.").

72. *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) (ruling that a plaintiff can establish sufficient injury to grant standing by satisfying either the "certainly impending" or "substantial risk" test).

73. *See* Clapper v. Amnesty Intern. USA, 568 U.S. 398, 410–14 (2013) (explaining the "certainly impending" test).

74. *See Clapper*, 568 U.S. at 414 n.5 (explaining the "substantial risk" test).

75. *See Driehaus*, 134 S. Ct. at 2341 (ruling that a plaintiff can establish sufficient injury to grant standing by satisfying either the "certainly impending" or "substantial risk" test).

76. *See* cases cited *supra* note 43 and accompanying text (illustrating the circuit split on the issue of standing in data breach cases).

77. *See In re* SuperValu, Inc., 870 F.3d 763, 771–72 (8th Cir. 2017) (finding that the threat of injury was too speculative to grant standing to plaintiffs whose data was stolen from defendant); *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011) (same); Beck v. McDonald, 848 F.3d 262, 276–77 (4th Cir. 2017) (finding that the threat of injury was too speculative to grant standing to plaintiffs whose data was illicitly accessed by third parties while in the care of the defending party).

an injury under law. However, when the Sixth, Seventh, and Ninth Circuits examined this legal issue, each found sufficient injury to confer standing.[78] As will be explained below, the significantly increased chances of future injury should be enough to satisfy the injury-in-fact requirement.

A. Cases That Failed to Find Standing

1. Beck v. McDonald[79]

The Fourth Circuit recently addressed this question in *Beck v. McDonald*.[80] On February 11, 2013, a laptop was stolen from Dorn VAMC's Respiratory Therapy Department.[81] The laptop contained unencrypted personal information of approximately 7,400 patients.[82] This personal information included names, birth dates, the last four digits of social security numbers, and certain physical descriptors.[83] Further investigation revealed that Dorn VAMC failed to follow standard policies and procedures to ensure safe

78. *See* Galaria v. Nationwide Mutual Insurance Comp., 663 F. App'x 384, 390–91 (6th Cir. 2016) (finding that there is sufficient injury to grant standing when a plaintiff's information is illegally stolen from the defending party); *see also* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 696 (7th Cir. 2015) (finding the injury requirement satisfied when a plaintiff's information is illegally stolen from the defending party because there is a "substantial risk" that future harm will occur (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (internal quotation marks omitted))); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) ("If a plaintiff faces 'a credible threat of harm' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III . . . . On these facts . . . Plaintiffs . . . have sufficiently alleged an injury-in-fact for purposes of Article III standing." (first quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002); and then quoting City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1938))); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) (finding sufficient injury to grant standing for plaintiffs whose information was hacked from defendant, particularly noting the costs plaintiffs incurred to mitigate future damages).

79. Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

80. *See generally id.* (finding that the threat of injury was too speculative to grant standing to plaintiffs whose data was illicitly accessed by third parties while in the care of the defending party).

81. *Id.* at 267.

82. *Id.*

83. *Id.*

storage of patient information.[84] In response, Richard Beck and Lakeshia Jeffery, two individuals whose information was exposed, filed a class action lawsuit.[85]

In July 2014, a similar fact pattern occurred: Four boxes were discovered missing, again from Dorn VAMC.[86] Those reports contained identifying information of over 2,000 patients, including names, social security numbers, and medical diagnoses.[87] In response, Beverly Watson, an individual whose information was now exposed, brought a separate class action lawsuit.[88]

In both cases, the claims were dismissed for want of standing, relying upon *Clapper*'s explanation on how future injury can convey standing.[89] Both Beck and Watson appealed to the Fourth Circuit and their appeals were consolidated to the present case.[90] Their argument was that the increased risk of future identity theft is sufficient injury or, in the alternative, the cost of protecting against the same is also sufficient injury.[91]

The Fourth Circuit began by examining the requirements of standing, focusing on the injury-in-fact requirement.[92] The court noted at the offset that "threatened rather than actual injury can satisfy Article III standing requirements."[93] However, "not all threatened injuries constitute an injury-in-fact."[94] Ultimately, the Fourth Circuit focused its analysis on whether either alleged "injury"—the data breach itself or the cost to protect against future identity theft—was a "distinct and palpable [injury], as opposed to [a] merely abstract [one.]"[95]

---

84. *Id.*

85. *Id.*

86. *Id.* at 268.

87. *Id.*

88. *Id.*

89. *See id.* at 268–69 (ruling the *Beck* plaintiffs lacked standing under the Privacy Act).

90. *Id.*

91. *See id.* at 273 (discussing Petitioner's argument that increased risk of future identity theft and the cost of protecting against it constitutes injury).

92. *See id.* at 270 ("We focus our inquiry on the first element of Article III standing: injury-in-fact.").

93. *Id.* at 271 (citing Friends of the Earth, Inc. v. Gaston Copper Recycling, Corp., 204 F.3d 149, 160 (4th Cir. 2000) (en banc)).

94. *Id.*

95. *Id.* (citing Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)).

Turning first to the increased risk of future identity theft, the Fourth Circuit noted the deepening circuit split on this issue.[96] The court then differentiated the current case from the cases where standing was found by ruling that in the other cases, the hacker "intentionally targeted the personal information compromised in the data breaches" as opposed to this fact pattern.[97] Specifically, the Fourth Circuit looked at four cases where standing was found: *Galaria v. Nationwide Ins. Comp.*,[98] *Remijas v. Neiman Marcus Group, LLC*,[99] *Pisciotta v. Old Nat. Bancorp*,[100] and *Krottner v. Starbucks Corp*.[101] The court pointed out that in *Galaria*, "hackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others," which did not happen here.[102] In *Remijas*, the Fourth Circuit noted that the only logical conclusion for hackers to break into a store's database and steal consumer private information is to target personal information; again, the Fourth Circuit said this is not present here.[103] In *Pisciotta*, the court said that the "scope and manner of intrusion into [the] banking website's hosting facility was sophisticated, intentional, and malicious," which, according to the Fourth Circuit, did not happen here.[104] Lastly, in "*Krottner*, at least

---

96. *Id.* at 273 ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft.").

97. *Id.* at 274.

98. *See* Galaria v. Nationwide Ins. Comp., 663 Fed. App'x 384, 391 (6th Cir. 2016) (ruling that plaintiffs have Article III standing to bring their action involving a data hack).

99. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 697 (7th Cir. 2015) (ruling that customers have Article III standing to bring their action by showing a substantial risk of harm from the store's date breach).

100. *See* Pisciotta v. Old Nat. 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 have otherwise faced, absent the defendant's actions.").

101. *See id.* (comparing the present case with other cases that addressed the same legal question).

102. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (citing Galaria v. Nationwide Insurance Comp., 663 Fed. App'x 384, 386 (6th Cir. 2016)).

103. *See id.* ("In . . . *Remijas*, . . . the data thief intentionally targeted the personal information compromised in the data breaches. . . . Here, the Plaintiffs make no such claims.") (citing Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015)).

104. *Id.* (internal quotations omitted) (citing Pisciotta v. Old Nat. Bancorp,

one named plaintiff alleged misuse or access of that personal information [stolen] by the thief," implying the hacker targeted the information used.[105] As of the Fourth Circuit's decision, there had not been a case of identity theft yet in *Beck*.[106]

Ultimately, the Fourth Circuit concluded that the data thief in *Beck* did not target the laptop, or boxes, for its personal information and, therefore, the increased chance of future identity theft is not a sufficient enough injury-in-fact to confer standing.[107] Notwithstanding the fact that the laptop was deemed to have been stolen, the court focused on the concept that an "attenuated chain of possibilities" would have to occur for Plaintiffs to be subject to identity theft.[108] Such "attenuated chain of possibilities" is not sufficient to confer standing.[109]

Having walked through the "certainly impending" test, the Fourth Circuit continued by analyzing the "substantial risk" standard set forth by *Clapper*.[110] The Plaintiffs alleged that 33% of those affected will become victims of identity theft.[111] The court, however, quickly devalued that argument by interpreting *Clapper* as setting an incredibly high bar to reach in order to obtain standing requirement.[112] Consequently, Plaintiffs were found to

---

499 F.3d 629, 632 (7th Cir. 2007)).

105. *See id.* ("[N]amed plaintiff alleged that, two months after theft of laptop containing his social security number, someone attempted to open a new account using his social security number." (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir. 2010)).

106. *See id.* (concluding that no plaintiff has alleged that her data has been stolen).

107. *See id.* ("Here, the Plaintiffs make no such claims [of the data thief intentionally targeting the personal information or of misuse of stolen data by the thief]. This in turn renders their contention of an enhanced risk of future identity theft too speculative.").

108. *See id.* at 275 ("[F]or the Plaintiffs to suffer the harm of identity theft . . . we must engage with the same 'attenuated chain of possibilities' rejected by the [U.S. Supreme] Court in *Clapper*." (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147–48 (2013))).

109. *See id.* (same).

110. *See id.* ("Nonetheless, our inquiry on standing is not at an end, for we may also find standing based on 'substantial risk' that the harm will occur, which in turn may prompt a party to reasonably incur costs to mitigate or avoid that harm." (quoting *Clapper*, 133 S. Ct. at 1150 n.5)).

111. *Id.* at 275–76.

112. *See id.* at 276 ("[W]e read *Clapper*[] . . . to express the common-sense notion that a threatened event can be 'reasonably likely' to occur but still be

not have satisfied the injury requirement of standing with the increased risk of future identity theft.[113]

The Fourth Circuit briefly looked at Plaintiff's second argument: The cost of mitigative measures is sufficient injury to confer standing.[114] However, that argument was summarily rejected as the court said, "[these] self-imposed harms cannot confer standing."[115] Accordingly, the Fourth Circuit found that Plaintiffs did not have standing here to sue.[116]

2. In re SuperValu, Inc.[117]

A similar legal issue was posed to the Eight Circuit in *In re SuperValu, Inc.*[118] SuperValu, Inc. [hereinafter "SuperValu"] was the victim of two cyberattacks in 2014.[119] The first occurred from June 22, 2014 to July 17, 2014.[120] During that time, hackers installed malicious software on SuperValu's computers that allowed them to gain access to and then steal the payment information of SuperValu's customers.[121] This included the customer's names, credit or debit card account numbers, expiration dates, card verification value codes, and personal identification numbers.[122] On August 14, 2014, SuperValu issued a press release

---

insufficiently 'imminent' to constitute an injury-in-fact."(citing *Clapper*, 133 S. Ct. at 1147–48)).

113. *See id.* (finding that none of the arguments set forth by Plaintiffs regarding the increased risk of future harm is sufficient injury to grant standing).

114. *See id.* at 276–77 ("Next, we turn to the Plaintiffs' allegation that they have suffered an injury-fin-fact because they have incurred or will in the future incur the cost of measures to guard against identity theft, including the costs of credit monitoring services.").

115. *Id.*

116. *See id.* (affirming the district court's conclusion that Plaintiffs did not have standing to pursue their claims).

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

118. *See id.* at 770–72 (discussing whether the increased risk of future identity theft stemming from a data breach is sufficient to grant standing to those whose information was stolen).

119. *Id.* at 766.

120. *Id.*

121. *Id.*

122. *Id.*

notifying customers of the intrusion.[123] SuperValu also noted that they were conducting an on-going investigation into the incident.[124]

On September 29, 2014, SuperValu announced that a second data breach took place in late August or early September 2014.[125] According to the release, the second data breach[126] involved an intruder installing malicious software onto the same system that was compromised in the first data breach.[127] This second type of malicious software achieved the same end goals as the first: Allow the hackers to have access to customers' personal card information.[128]

After the two press releases, Plaintiffs filed suit claiming SuperValu failed to take adequate measures to protect customers' card information.[129] Because of that failure, Plaintiffs argued that they were subjected to an imminent and real possibility of identity theft.[130] Specifically, the thieves would siphon money from the customers' various accounts, open new accounts, or sell the information to others who intend to commit fraud.[131] In fact, one of the Plaintiffs alleged that there were already fraudulent charges on his credit card statement stemming from the initial data breaches.[132] The district court dismissed the complaint, "finding

123. *Id.*

124. *Id.*

125. *Id.*

126. SuperValu claimed the two breaches were separate, but the Plaintiffs disputed that contention in their complaint. *Id.* It is irrelevant to this note which sequence of events is correct.

127. See *id.* ("The press release stated that an intruder installed different malicious software onto the same network.").

128. *See id.* ("Defendants acknowledged that the software may have captured Card Information from debit and credit cards used to purchase goods at their stores, but at the time of the press release, there had been no determination that such information was 'in fact stolen.'").

129. *Id.*

130. *Id.*

131. *Id.* at 766–67.

132. *See id.* at 767 ("Shortly after the data breach was announced, 'Holmes noticed a fraudulent charge on his credit card statement and immediately cancelled his credit card, which took two weeks to replace.'").

that none of the plaintiffs had alleged an injury-in-fact and thus did not have standing."[133] Plaintiffs appealed.[134]

The Eighth Circuit began its analysis by reiterating the abecedarian principles of Article III standing: Injury, causation, and redressability.[135] In particular, the Eighth Circuit, like the Fourth Circuit, analyzed the injury requirement.[136] Put another way, the court analyzed "whether Plaintiffs' allegations plausibly demonstrate that the risk that plaintiffs will suffer future identity theft is substantial."[137] At the outset, the Eighth Circuit concluded that the plaintiffs sufficiently alleged that their card information was stolen by the hackers.[138] The court then noted that the plaintiff who alleged fraudulent credit card transactions, Holmes, had sufficient injury.[139] However, the Eighth Circuit concluded that the other plaintiffs failed to allege an injury-in-fact with the increased risk of future harm.[140] This conclusion hinged upon a government report analyzing data breaches and their aftermaths.[141]

The Eight Circuit first noted, using the government report mentioned above, that the information stolen would not allow for someone to open new bank accounts without the proper owner's knowledge.[142] The court continued by concluding that the findings of the GAO report indicate that the odds of someone's identity

---

133. *Id.*

134. *Id.*

135. *See id.* at 767–78 (discussing the elements of constitutional standing).

136. *See id.* at 768 ("This case primarily concerns the injury in fact . . . element.").

137. *Id.* at 770.

138. *See id.* at 770 ([W]e are satisfied that the complaint sufficiently alleges that the hackers stole plaintiffs' Card Information.").

139. *See id.* at 772 ("[P]laintiff Holmes alleges a present injury in fact to support his standing.").

140. *See id.* at 771–72 ("Accordingly, we conclude that the complaint has not sufficiently alleged a substantial risk of identity theft, and Plaintiffs' allegations of future injury do not support standing in this case.").

141. *See id.* at 770–71 (dissecting a 2007 Government Accountability Office report on data breaches and determining that it fails to support plaintiffs' contention of sufficient increased risk of future injury) (citing U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) [hereinafter "GAO report"]).

142. *See id.* at 770 ("As the GAO report points out, compromised credit or debit card information, like the Card Information here, generally cannot be used alone to open unauthorized new accounts." (internal citations omitted)).

being taken is too small to satisfy the constitution's requirements for injury-in-fact.[143] However, the court also noted that the GAO report found that "comprehensive information on the outcomes of data breaches is not available . . . and the extent to which data breaches result in identity theft is not well known."[144] Notwithstanding these informational defects within the GAO report, the court concluded that the GAO report proves that the increased risk of future injury was too speculative to grant standing.[145]

3. Reilly v. Ceridian Corp.[146]

The Third Circuit also analyzed this legal issue in *Reilly v. Ceridian Corp.*[147] In that case, Ceridian Corp. suffered a security breach when an unknown hacker infiltrated the company's payroll system.[148] This breach exposed personal and financial information of approximately 27,000 employees at 1,900 companies.[149] However, the Court noted that hackers may not have read, copied, or understood the data.[150] When Ceridian learned of the data breach, they informed the victims, and this suit followed.[151]

Plaintiffs filed a class action, alleging that they were injured by, "an increased risk of identity theft, . . . incurred costs to monitor their credit activity, and . . . emotional distress."[152] Like the two previous cases mentioned above, the district court

---

143. *See id.* at 771 (discussing the report's findings on how many data breaches are known to have caused identity theft, ultimately concluding that the report "does not support the allegation that [SuperValu's] data breaches create a substantial risk that plaintiffs will suffer credit or debit card fraud").

144. *Id.* at 771 (internal quotation marks omitted) (citing GAO report at 21).

145. *See id.* at 771–72 ("Accordingly, we conclude that the complaint has not sufficiently alleged a substantial risk of identity theft, and plaintiffs' allegations of future injury do not support standing in this case.").

146. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

147. *See generally id.* (affirming the District Court's determination that the plaintiffs' allegations were insufficient to plead actual injury and therefore lacked standing).

148. *Id.* at 40.

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.*

dismissed Plaintiffs' claims for want of standing.[153] Plaintiffs appealed.[154]

In its inquiry, the Third Circuit also focused on the injury requirement of standing.[155] Particularly, the Third Circuit highlighted the limiting nature of the injury requirement, stating, "[a]llegations of possible future injury are not sufficient to satisfy Article III."[156] The Third Circuit quickly concluded that Plaintiffs "allegations of hypothetical, future injury are insufficient to establish standing."[157] Furthermore, they indicated that to succeed, the Plaintiffs must have alleged, and later proved, that the hacker, "(1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs'] names."[158]

In its rationale, the Third Circuit distinguishes this case from two similar cases where sister circuits had found standing: *Pisciotta v. Old Nat'l Bancorp*[159] and *Krottner v. Starbucks Corp.*[160].[161] The Third Circuit attempted to differentiate itself from *Pisciotta* by saying, "there was evidence that the hacker's intrusion was sophisticated, intentional and malicious [in that case]."[162] The Third Circuit then ruled that this was not present here.[163] In *Krottner*, there was an attempt "to open a bank account with a plaintiff's information following the physical theft of a laptop."[164] Again, the Third Circuit ruled this was not present here.[165]

---

153. *Id.* at 41.

154. *Id.*

155. *See id.* ("Constitutional standing requires an injury-in-fact, which is an invasion of a legally protected interest.").

156. *Id.* at 42 (internal citations omitted).

157. *Id.*

158. *Id.*

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

160. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

161. *See Reilly*, 664 F.3d at 43–44 (explaining how *Pisciotta* and *Krottner* are different than the case at hand).

162. *Id.* at 44 (citing *Pisciotta*, 499 F.3d at 632).

163. *See id.* ("Here, there is no evidence that the intrusion was intentional or malicious.").

164. *Id.* (citing *Krottner*, 628 F.3d at 1142).

165. *See id.* ("[Plaintiffs] have alleged no misuse.").

Lastly, the Third Circuit rejected the argument that Plaintiffs' purchase of identity theft protection is sufficient injury.[166] Instead, the Third Circuit explained it away as merely "[Plaintiffs] prophylactically spen[ding] money to ease fears of future third-party criminality."[167] Ultimately, the Third Circuit concluded, in affirming the district court's dismissal: "[T]here is no quantifiable risk of damage in the future . . . . Any damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker."[168]

B. Cases that Find Standing

1. Galaria v. Nationwide Mutual Ins. Comp.[169]

Multiple Circuit Courts have come to the opposite opinion of the Fourth, Eighth, and Third Circuits regarding whether increased risk of identity theft is enough of an injury in these types of cases.[170] In *Galaria v. Nationwide Mutual Ins. Comp.*, hackers breached Nationwide Mutual Insurance Company's firewall and accessed personal information.[171] This personal information included names, dates of birth, marital statuses, genders, occupations, employers, social security numbers, and driver's license numbers.[172] Plaintiffs brought suit and alleged that the Nationwide breach created an "imminent, immediate and continuing risk" that Plaintiffs and other class members would be subject to identity fraud.[173] Indeed, Plaintiffs pointed to a study that concluded, "in 2011 recipients of data-breach notifications

166. *See id.* at 45 ("Although [Plaintiffs] have incurred expenses to monitor their accounts and to protect their personal and financial information from imminent misuse and/or identity theft, they have not done so as a result of any actual injury.").

167. *Id.*

168. *Id.*

169. Galaria v. Nationwide Mutual Ins. Comp., 63 F. App'x 384 (6th Cir. 2016).

170. *See* cases cited *supra* note 43 and accompanying text (listing the circuit split).

171. *Galaria*, 663 F. App'x at 388.

172. *Id.*

173. *Id.* at 386.

were 9.6 times more likely to experience identity fraud, and had a fraud incidence rate of 19%."[174] Beyond that, Plaintiffs alleged that they wanted to mitigate this risk of identity fraud by paying an average of $354 in out-of-pocket expenses and $1513 in total economic loss to obtain identity theft protection.[175] It was through these two major reasons—increased risk of future injury and the mitigation costs to avoid such future injury—that Plaintiffs claimed they had satisfied the constitutional requirements of standing.[176] The district court rejected these arguments and the Plaintiffs appealed their case to the Sixth Circuit.

The Sixth Circuit began its analysis by reiterating the principles of constitutional standing, taking particular note of the injury requirement.[177] The court also took particular note of the Supreme Court's jurisprudence regarding when future injury satisfies the injury requirement of constitutional standing.[178] With this in mind, the Sixth Circuit concluded that "Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of litigation."[179] The Sixth Circuit pointed out that there is a presumption that when information is stolen, it is presumed that it will be used for nefarious purposes, such as stealing someone's identity.[180] Consequently, even though the injury is not "literally certain," there is a "sufficiently substantial risk of harm" that the injury will occur.[181]

With the injury requirement satisfied, the Sixth Circuit moved to the other two requirements of constitutional standing:

---

174. *Id.*

175. *Id.*

176. *Id.* at 386–87.

177. *See id.* at 388 ("Injury is the first and foremost of standing's three elements.") (internal citation omitted).

178. *See id.* (explaining that a substantial risk that future harm will occur is sufficient to fulfil constitutional standing).

179. *Id.*

180. *See id.* at 388, 389 ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals . . . . Presumably, the purpose of the hack is, sooner or later, to make a fraudulent charge or assume those consumers' identities.").

181. *Id.* at 388.

Causation and redressability.[182] The court, however, quickly flew through those two requirements and concluded they were satisfied.[183] The Sixth Circuit then reversed the district court's determination that Plaintiffs did not have standing and remanded.[184]

2. Remijas v. Neiman Marcus Group, LLC[185]

The Seventh Circuit also discussed a similar legal issue in *Remijas v. Neiman Marcus Group, LLC*.[186] The facts of that case are as follows. Sometime in 2013, hackers attacked Neiman Marcus Group, LLC [hereinafter "NMG"] and stole some of their customers' credit card information.[187] In December of that year, NMG learned of fraudulent charges showing up on some of its customers' credit cards.[188] However, NMG kept that information confidential until January the following year.[189] The company then announced that around 350,000 cards had been exposed and approximately 9,200 had already been fraudulently used.[190] The Plaintiffs here quickly filed suit.[191] The district court dismissed the claim for want of standing.[192] Plaintiffs appealed.[193]

The Seventh Circuit undertook the same analysis as the Sixth Circuit had taken regarding the increased chance of both future injury and current injury.[194] In regard to the heightened risk of

182. *See id.* at 390–91 (explaining that the injury must be caused by the defendants and a favorable decision must be able to redress the injury).

183. *See id.* (explaining that Plaintiff's injury was caused by the defendant and a favorable decision would redress the injury).

184. *See id.* ("Thus, we conclude that Plaintiffs' complaints adequately allege Article III standing.").

185. Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015).

186. *See id.* at 689–70 (finding that the plaintiff's showing of a substantial risk of harm from the store's data breach satisfied Article III's injury requirement).

187. *Id.* at 689.

188. *Id.* at 690.

189. *Id.*

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.*

194. *See id.* at 692 ("These plaintiffs must allege that the data breach

future injury, the Seventh Circuit came to a number of conclusions, including:

> [R]equiring the plaintiffs to wait for the threatened harm to materialize in order to sue would create a different problem: [T]he more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not fairly traceable to the defendant's data breach.[195]

The court then noted a Government Accountability Office Report which concluded that "stolen 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."[196] So, the fact that only 9,200 cards have been compromised so far does not preclude the significant possibility that more could be injured in the future.[197] For these reasons, coupled with the presumption that the hacker's intentions were nefarious, the Seventh Circuit concluded that there is sufficient injury to grant standing under the "certainly impending" test.[198]

The Seventh Circuit, however, continued to analyze if Plaintiffs' purchasing of identity theft protection was sufficient.[199] The court noted that "[p]laintiffs cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[200] However, as noted above, the Seventh Circuit concluded that the future harm was imminent; therefore, these mitigation costs also constitute sufficient injury to confer standing.[201]

---

inflicted . . . injury on them; that [Defendant] caused that injury; and that a judicial decision can provide redress for them.").

195. *Id.* at 693.

196. *Id.* at 694.

197. *See id.* ("[T]he complaint asserts that fraudulent charges and identity theft can occur long after a data breach.").

198. *See id.* at 693 ("[P]laintiffs have shown a substantial risk of harm from the [Defendant's] data breach. Why else would hackers break into a store's database and steal consumers' private information?").

199. *See id.* at 694 ("In addition to the alleged future injures, the plaintiffs assert that they have already lost time and money protecting themselves against future identity theft and fraudulent charges.").

200. *Id.*

201. *See id.* ("An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring.").

Lastly, the Seventh Circuit mentioned an issue that every other case had not even addressed: Is private information property?[202] While the Seventh Circuit bypassed the question and dismisses it because the Plaintiffs did not provide any authority that would support such a conclusion, it is an interesting proposition.[203]

3. Krottner v. Starbucks Corp.[204]

The Ninth Circuit dealt with an analogous legal issue in *Krottner v. Starbucks Corp.*[205] The facts of that case are as follows. In October 2008, someone stole a laptop from Starbucks that contained the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees.[206] In November of that year, Starbucks sent a letter to those affected, alerting them to the theft and stating that Starbucks had "no indication that the private information had been misused."[207] However, Starbucks still told those affected to closely monitor their financial accounts for suspicious activity and provided credit watch services for the next year.[208] Two of the Plaintiffs continued to pay out-of-pocket for continued credit watch services after the one year of free service concluded and, arguably because of the continued surveillance, they had not yet suffered any sort of identity theft at the time of the Ninth Circuit's decision.[209] Indeed, there was an attempt to open a bank account in one of the Plaintiff's name and social security number, but the bank closed the account before any damage could be done.[210] Plaintiffs then brought a class action

202. *See id.* at 695 ("The plaintiffs also allege that they have a concrete injury in the loss of their private information, which they characterize as an intangible commodity.").

203. *See id.* ("Plaintiffs refer us to no authority that would support such a finding. We thus refrain from supporting standing on such an abstract injury.").

204. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

205. *See id.* at 1142 ("Plaintiffs-Appellants' remaining allegations concern their increased risk of future identity theft.").

206. *Id.* at 1140.

207. *Id.* at 1140–41.

208. *See id.* at 1141 (referencing a letter Starbucks sent out to those affected).

209. *Id*.

210. *Id.*

against Starbucks.[211] The district court dismissed the complaint for failing to allege a cognizable injury under law.[212] Plaintiffs appealed.[213]

The Ninth Circuit began by reanalyzing the district court's determination of Article III standing.[214] Again, the court focused on the injury requirement.[215] In particular, whether the increased risk of future identity theft is sufficient even though there has not been any actual loss yet.[216] The court compared this increased risk of future harm to environmental and toxic exposure claims, which have legally similar injuries to data breach cases due to a delay in occurrence and some uncertainty that injury will ever occur.[217] Ultimately, the Ninth Circuit concluded that "Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[218] However, the Ninth Circuit qualified this result by indicating that if the allegations were more conjectural or hypothetical, such as if the laptop had not been stolen, but it had been at risk of being stolen at some point, there would be no standing.[219]

---

211. *Id*.

212. *Id.*

213. *Id.*

214. *See id.* ("We have an independent obligation to examine standing to determine whether it comports with the case or controversy requirement of Article III, Section 2 of the Constitution.").

215. *See id.* at 1141–42 ("It was undisputed before the district court that Plaintiffs-Appellants had sufficiently alleged causation and redressability, the second and third standing requirements. We thus turn to the first standing requirement: [W]hether Plaintiffs-Appellants adequately alleged an injury-in-fact.").

216. *See id. at* 1142 (explaining the arguments by Plaintiff trying to establish standing).

217. *See id.* (concluding that environmental and toxic exposure claims are similar because, like the current case, the injury is neither occurring presently nor guaranteed to ever occur, but the increased likelihood to cause future injury is sufficient to grant standing) (citing Cent. Delta Water Agency v. United States, 306 F.3d 938, 948–50 (9th Cir. 2002) (adjudicating an environmental claim) & Pritikin v. Dep't of Energy, 254 F.3d 791, 796–97 (9th Cir. 2001) (adjudicating a toxic exposure claim)).

218. *Id.* at 1143.

219. *See id.* ("Were Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible.").

4. Attias v. Carefirst, Inc.[220]

The most recent circuit court to deal with this legal issue was the D.C. Circuit in *Attias v. Carefirst, Inc.*[221] In that case, health insurer CareFirst, Inc. suffered a cyberattack in which its customers' personal information was allegedly stolen.[222] This personal information included names, birthdates, email addresses, social security numbers, and credit card information.[223] The attack occurred in June 2014, and the breach was discovered in April 2015.[224] The affected individuals were then informed of the breach in May, 2015.[225] Plaintiffs soon after brought a class action lawsuit against CareFirst, alleging a number of different causes of action.[226] The district court dismissed the complaint for want of standing.[227] The Plaintiffs quickly filed an appeal.[228]

The D.C. Circuit began by highlighting the injury-in-fact requirement of constitutional standing.[229] Specifically, whether the future injury alleged by Plaintiffs is "actual or imminent" enough to confer standing.[230] For that, the D.C. Circuit focused on the "substantial risk" test.[231]

Courts around the country have separately molded the various future injury tests that the Supreme Court discussed in *Clapper* and its progeny.[232] In the D.C. Circuit, the appropriate method of analyzing an "increased-risk-of-harm claim is to consider the

220. Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

221. *See generally id.* (grappling with the legal question of whether data breaches are sufficient to grant standing to those affected).

222. *Id.* at 622.

223. *Id.* at 623.

224. *Id.*

225. *Id.*

226. *Id.*

227. *Id.*

228. *Id.*

229. *See id.* at 626 ("This case primarily concerns the injury-in-fact requirement.").

230. *Id.* ("An injury in fact must be concrete, particularized, and, most importantly for our purposes, 'actual or imminent' rather than speculative.") (internal citations omitted).

231. *See id.* at 627 (discussing the "substantial risk" test of injury).

232. *See, e.g.*, *id.* (discussing the D.C. Circuit's precedent regarding the "substantial risk" test); *see also* cases cited *supra* notes 72–75 and accompanying text (explaining the various future injury-in-fact tests).

ultimate alleged harm,' which in this case would be identity theft, 'as the . . . injury[,] and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently imminent for standing purposes.'"[233] Accordingly, the inquiry then turned to whether the plaintiffs sufficiently alleged that there is a "substantial risk of identity theft as a result of defendant's alleged negligence."[234] The D.C. Circuit analyzed the complaint and concluded that there is "[n]o long sequence of uncertain contingencies involving multiple independent actors [that must] occur before the plaintiffs in this case will suffer any harm."[235] The D.C. Circuit continues, stating, "simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken . . . . [Plaintiffs] satisfy the requirement of an injury in fact."[236] With the injury requirement satisfied, the D.C. Circuit quickly disposed of the other standing requirements and ruled that the Plaintiffs have standing to pursue their claims.[237]

III. Why Courts Should Find the Increased Threat of Future Injury Justifies Standing in These Types of Cases

In *Beck*, *In re SuperValu, Inc.*, and *Reilly* ("Non-Standing Cases") there were two common threads of error that *Galaria*, *Remijas*, *Krottner*, and *Attias* ("Standing Cases") do not have. First, the Non-Standing Cases' incorrectly assumed that hackers' intent may not be malicious.[238] Second, the Non-Standing Cases improperly focused on the whether any identity theft has occurred, rather than focusing on the complexities of the hacking attack.[239]

---

233. *Id.* (quoting Food & Water Watch v. Vilsack, 808 F.3d 905, 915 (D.C. Cir. 2015)).

234. *Id.*

235. *Id.* at 629.

236. *Id.*

237. *See id.* at 629–30. (describing why the plaintiffs have standing).

238. *See* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) ("[P]laintiffs have uncovered no evidence that . . . the thief stole the laptop with the intent to steal their private information."); *see also In re* SuperValu, Inc., 870 F.3d 763, 769 (8th Cir. 2017) (requiring Plaintiffs to specifically allege that their information was stolen instead of presuming it); Reilly v. Ceridian, 664 F.3d 38, 44 (3d Cir. 2011) ("Here, there is no evidence that the intrusion was intentional or malicious.").

239. *See Beck*, 848 F.3d at 275 (focusing on whether future identity theft has

Instead, the hacking event, by itself, should confer a presumption that there is a sufficiently increased chance of future injury so as to grant standing.

A. Courts Should Presume that the Hacker is Planning to Misuse the Stolen Data Because Hacking Is a Difficult and Illegal Activity

Turning to the first common error, the Non-Standing Cases failed to assume that the hacker had ill-intent in stealing the information.[240] This is incorrect.

Hacking a database, particularly overcoming the high level of security the defendants in these cases presumably apply, is especially difficult.[241] Two of the most common types of attacks utilized for this special purpose are brute force attacks and trojan viruses.[242] Both of these methods are neither cheap nor simple, requiring a large investment of time.[243]

---

occurred); *see also In re SuperValu, Inc.*, 870 F.3d at 769–71 (discussing the potential future injury from the hacking); *Reilly*, 664 F.3d at 43 (same).

240. *See Beck*, 848 F.3d at 274 ("[P]laintiffs have uncovered no evidence that . . . . [T]he thief stole the laptop with the intent to steal their private information."); *see also In re SuperValu, Inc.*, 870 F.3d at 769 (requiring Plaintiffs to specifically allege that their information was stolen before beginning a standing analysis); *Reilly*, 664 F.3d at 44 ("Here, there is no evidence that the intrusion was intentional or malicious.").

241. *See* CESAR CERRUDO & ESTEBAN MARTINEZ FAYO, HACKING DATABASES FOR OWNING YOUR DATA 4–6 (2007), https://www.blackhat.com/presentations/bh-europe-07/Cerrudo/Whitepaper/bh-eu-07-cerrudo-WP-up.pdf (explaining the various ways that hackers illegally access databases and the difficulty of performing such hacks) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

242. *See id.* at 4–5 (describing how databases are hacked and different methods that hackers use).

243. *See How to Crack Passwords, Part 1 (Principles & Technologies)*, NULL BYTE (May 26, 2016, 3:15 PM), https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/ [hereinafter *How to Crack Passwords*] (describing how expensive and complicated brute force attacks are) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* SebastianZ, *Security 1:1 - Part 2 - Trojans and Other Security Threats*, SYMANTEC (Dec. 26, 2013), https://www.symantec.com/connect/articles/security-11-part-2-trojans-and-other-threats ("Trojans are generally created by malware authors who are organized and aim to make money out of their efforts. These types of Trojans can be highly sophisticated and can require more work to implement than some of the simpler malware seen on the Internet.") (on file with

A brute force attack is a term used to reference an illegal retrieval of passwords.[244] It has a simple premise: Attempt all possible combinations of letters, numbers, and symbols until the correct password is found.[245] However, this attack is not always an attempt to discover the actual database password, as enterprises generally have security against this, but rather, it is generally an attempt to decrypt the password file.[246] This type of brute force attack is called "breaking the hash."[247] Put another way, let us say you are attempting to break into a vault.[248] This vault requires a key to enter.[249] If you tried to pick the vault lock a million times, the lock would break and restrict access to the vault.[250] However, next to the entrance of the vault is a safe containing the key necessary to enter the vault.[251] So, you decide to take the safe home and attempt to find the combination.[252] You try every single combination on the safe and, eventually, it clicks open to reveal the key inside.[253] You take the key and enter the vault.[254] This is, conceptually, how a "breaking the hash" brute force attack is performed.[255] The vault is the database that contains the personal information the hackers seek.[256] The key is the password needed

---

the Washington & Lee Journal of Civil Rights & Social Justice).

244. *See How to Crack Passwords*, *supra* note 243 (describing what brute force attacks are and how they occur).

245. *See id.* ("Brute force password cracking attempts all possibilities of all the letters, number, special characters that might be combined for a password and attempts them.").

246. *See id.* (describing methods of "cracking" passwords).

247. *See Introduction to Cracking MD5 Encryption—Breaking the Hash Functions,* BREAKING THE SECURITY (Feb. 16, 2011), http://breakthesecurity.cysecurity.org/2011/02/introduction-to-cracking-md5-encryption- breaking-the-hash-functions.html (explaining the term "breaking the hash") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

248. *Cf. How to Crack Passwords*, *supra* note 243 (describing what brute force attacks are and how they occur).

249. *Cf. id.* (same).

250. *Cf. id.* (same).

251. *Cf. id.* (describing how a password is protected).

252. *Cf. id.* (referencing how hackers work to decode passwords).

253. *Cf. id.* (noting the process hackers use).

254. *Cf. id.* (same).

255. *Cf. id.* (same).

256. *Cf. id. (*same).

to open the database.[257] The safe protecting the key is the encryption utilized on the password.[258] Lastly, the combination to open the safe is the encryption key to decrypt the sought after database password.[259] While this is just one type of brute force attack, this analogy shows that the execution of any brute force attack is incredibly complex.[260]

On top of the intricacy of a brute force attack, it is also expensive and time consuming.[261] Most passwords today are encrypted with 256-bit encryption.[262] The number "256" refers to the size of the encryption key, or the length of the "combination," using the analogy above.[263] Put numerically, there are 2^{256} possible combinations that the decryption "combination" could be.[264] With that many possible combinations, a hacker could not feasibly sit for years and type each one in. Instead, the hacker would either download software to do it for her or, if she is sophisticated enough, develop her own software.[265] Regardless, she then needs the raw computing power to run the software quickly, so as to make the "decryption" process efficient enough to be valuable.[266] Amateur hackers will usually purchase bot nets, which spread the processing power over millions of machines, or purchase

---

257. *Cf. id.* (same).

258. *Cf. id.* (same).

259. *Cf. id.* (same).

260. *See id.* (explaining the complexity of brute force attacks).

261. *See id.* (describing the cost and time investment required to effectuate a brute force attack).

262. *See* David Bisson, *The Evolution of 256-bit Encryption and Security Certificates*, VENAFI (Sept. 8, 2017), https://www.venafi.com/blog/evolution-256-bit-encryption-and-security-certificates ("Most organizations require their employees use AES 256-bit encryption.") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

263. *See 256-Bit Encryption*, TECHOPEDIA, https://www.techopedia.com/definition/29703/256-bit-encryption (last visited Feb. 21, 2018) ("256-bit encryption is refers to the length of the encryption key used to encrypt a data stream or file") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

264. *See id.* ("A hacker or cracker will require 2256 different combinations to break a 256-bit encrypted message.").

265. *See How to Crack Passwords,* NULL BYTE, *supra* note 243 (listing the various software packages available to wannabe hackers, including "John the Ripper," "Ophcrack," and many others)

266. *See id.* (describing how much computer power is necessary to effectuate a brute force hack).

specialized equipment.[267] Both of these options are incredibly expensive.[268] For example, Black Arrow Software produces a special device that performs these type of brute force attacks.[269] It costs $350,000.[270] Consequently, the time and money investment to attack major corporations can be massive.[271] Because of this, very few individuals will attempt to hack enterprises unless they are seeking profit, either by selling the information to the highest bidder or the company is paying them to test the security.

The other database attack strategy mentioned above is to install a trojan horse virus within the system.[272] A trojan horse virus takes its name from the mythical trojan horse in the *Iliad*.[273] Like the mythical "horse," the virus presents itself as something familiar and attempts to remain undetected until activated by the hacker.[274] When the virus gets activated, it can do a number of things, depending on what its creator intends for it to do.[275] This could include opening a backdoor for the hacker, giving the hacker unfettered access to the network; scanning the system for passwords and valuable information; logging key strokes; and more.[276]

---

267. *See id.* (listing the possible ways that wannabe hackers will increase their computer power).

268. *See, e.g.*, *Scrypt ASICs*, BLACK ARROW INFO. TECH., http://www.blackarrowsoftware.com/store/litecoin-asics/ (last visited Feb. 21, 2018) (listing their brute force specialized machine for $350,000) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

269. *See id.* (same).

270. *See id.* (same).

271. *See, e.g.*, *id.* (same).

272. *See* CERRUDO & FAYO, *supra* note 241 (listing the most popular methods by which hackers illicitly access databases).

273. *See Trojan Horse Definition*, TECHTERMS, https://techterms.com/definition/trojanhorse (last visited Feb. 21, 2018) (defining the term "trojan horse" in the computer virus context) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

274. *See id.* ("Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer.").

275. *See id.* (detailing ways the trojan horse can infiltrate software).

276. *See, e.g.*, JAMIE CRAPANZANO, DECONSTRUCTING SUBSEVEN, THE TROJAN HORSE OF CHOICE 3 (2003) https://www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953 (detailing the Trojan Horse SubSeven's capabilities including, turning on webcams, abort programs, and usurp instant messaging services) (on file with the Washington &

As one could imagine, these trojan horse viruses are complicated to create and utilize.[277] The virus' code must account for the target's antivirus system[278], and, with large enterprises, these antivirus systems are usually advanced.[279] So, to counteract these heightened antiviruses, a trojan horse viruse would have to be coded to mutate itself into something else once it was downloaded onto the target computer so as to avoid detection.[280] This is known as polymorphic coding.[281] The sophistication of this coding generally requires that the code be custom-made for the hacker's target.[282] All of this takes *significant* amounts of time and skill.[283] Like with brute force attacks, the requisite costs involved in a trojan horse attack indicate that hackers who illicitly gain access to enterprise databases through trojan horse viruses presumptively intend to misuse the compromised data.

These two methods of attack are not the only ways by which a hacker could illegally access databases, but are some of the most common methods.[284] However, like the two examples presented above, each type of attack requires immense knowledge, time, and

---

Lee Journal of Civil Rights & Social Justice).

277. *See* SebastianZ, *supra* note 243 ("Trojans are generally created by malware authors who are organized and aim to make money out of their efforts. These types of Trojans can be highly sophisticated and can require more work to implement than some of the simpler malware seen on the Internet.").

278. Antivirus systems are incredibly complex, but they all distill down to comparing files or parts of files to known virus signatures. *See* Chris Hoffman, *How Antivirus Software Work*, HOW-TO-GEEK (Sept. 26, 2016), https://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/ (describing how anti-virus systems work) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

279. *See* AVAST SOFTWARE, INC., AVAST BUSINESS ENDPOINT PROTECTION SOLUTIONS - WINDOWS, 1–2 (2017) (listing the various enterprise antivirus capabilities).

280. *See Polymorphic Virus*, TECHOPEDIA, https://www.techopedia.com/definition/4055/polymorphic-virus (last visited Feb. 21, 2018) ("A polymorphic virus is a complicated computer virus that affects data types and functions. It is a self-encrypted virus designed to avoid detection by a scanner. Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

281. *See id.* (defining polymorphic viruses).

282. *Id*.

283. *See id.* (same).

284. *See* CERRUDO & FAYO, *supra* note 241 (listing the most popular methods by which hackers illicitly access databases).

money.[285] The difficulty and costs alone should indicate ill-intent when someone unlawfully accesses confidential databases.[286] Notwithstanding that, the Non-Standing Cases' opinions seems to imply that the hackers could have accidentally accessed this information.[287] Indeed, the Fourth Circuit in *Beck* specifically stated, "the . . . Plaintiffs have uncovered no evidence that the . . . thief stole the laptop with the intent to steal their private information."[288] It is unclear how the Plaintiffs in that case would have proven such a fact—being that the hacker was not known at the time—but, because of that, the Fourth Circuit ruled that there was no standing.[289] The Eight Circuit likewise concluded so in *In re SuperValu, Inc.*[290]

In *Reilly*, the Third Circuit egregiously focused on this false conclusion.[291] Again, the court in *Reilly* stated that on approximately December 22, 2009, "Ceridian suffered a security breach. An unknown hacker infiltrated Ceridian's Powerpay system and *potentially* gained access to personal and financial information belonging to Appellants and approximately 27,000 employees at 1,900 companies. It is *not known* whether the hacker read, copied, or understood the data."[292] The Third Circuit then

---

285. *See id.* (highlighting the difficulty of hacking corporate databases).

286. *Cf. id.* (same).

287. *See* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) ("[P]laintiffs have uncovered no evidence that . . . the thief stole the laptop with the intent to steal their private information."); *see also In re* SuperValu, Inc., 870 F.3d 763, 769 (8th Cir. 2017) (requiring Plaintiffs to specifically allege that their information was stolen instead of presuming it); Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011) ("Here, there is no evidence that the intrusion was intentional or malicious.").

288. *Beck*, 848 F.3d at 274.

289. *See id.* at 276 (concluding that for Plaintiffs to suffer harm, there must be an attenuated chain of events by third parties; this defeats standing).

290. *See In re* SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017) ("[O]thers have ruled that a complaint could plausibly plead that the theft of a plaintiff's personal or financial information [inherently] creates a substantial risk that they will suffer identity theft sufficient to constitute a[n] . . . injury . . . we conclude that plaintiffs have not done so here.").

291. *See Reilly*, 664 F.3d at 42 ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of appellants by making unauthorized transactions in Appellants' names.").

292. *Id.* at 40.

noted that Ceridian's own investigation determined that the threat was sufficient enough to send out letters to the affected individuals.[293] Nevertheless, the Third Circuit concluded that plaintiffs do not have standing because it is only "speculation" to think that the hacker got the information and then wanted to abuse it.[294] Ultimately, the Third Circuit said, "[a]ny damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker," even though the hackers clearly had enough skill to hack Ceridian's database to begin with.[295]

In the Non-Standing Cases, the courts' failures to presume that the hackers had ill-intent in hacking the various defendants' databases is incorrect, given the difficulty and costs of hacking.[296] Further buttressing this point, hacking itself is illegal.[297] While it remains *theoretically* possible that the hacker(s) in the Non-Standing Cases had no ill-intent; logically, this possibility is vastly outweighed by the large probability that the hacker(s) do have ill-intent. Why else would the hackers go to the trouble of performing the hack and expose themselves to criminal liability? The Seventh Circuit in *Remijas* put it well: "Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[298]

The procedural burden that some courts thrust upon prospective plaintiffs to prove that the hacker both copied and plans to misuse the data is not only unnecessary, as shown above,[299] it presents a nearly insurmountable burden. To prove

---

293. *See id.* ("Ceridian sent letters to the potential identity theft victims, informing them of the breach . . . .").

294. *See id.* at 42 ("Appellants' contentions rely on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of appellants by making unauthorized transactions in Appellants' names.").

295. *Id.* at 45.

296. *See* CERRUDO & FAYO, *supra* note 241 (explaining the difficulties associated with hacking).

297. *See* 18 U.S.C. § 1030 (2012) (stating that knowingly hacking without authorization is illegal).

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

299. *See supra* notes 241–88 and accompanying text (indicating that courts

that the hacker stole information, much less plans to misuse it, the plaintiffs would, at the very least, need access to the servers that were hacked.[300] They would then need to have an expert go over the data and see if there are any traces of copying left.[301] Sometimes there may not be.[302] The largest obstacle, however, is that they would need all of this before they got through the court doors.[303] The prospective plaintiffs would not have civil discovery powers, and the company is *certainly* incentivized to block access to avoid a lawsuit.[304] Either way, the plaintiffs are left penniless and holding the bag for something that they had nothing to do with and could not have stopped, even if they tried.

The Standing Cases' courts agreed with this argument.[305] The Sixth Circuit said in *Galaria*, "[w]here a data breach targets personal information, a reasonable inference can be drawn that the

---

should presume that hackers have ill intent when they hack an enterprise database).

300. *See How Do I Know if My Server has Been Hacked*, SERVERPRONTO: U. (July 08, 2015), https://www.serverpronto.com/spu/2015/07/how-do-i-know-if-my-server-has-been-hacked/ (listing the ways that someone can tell if her server has been hacked, all of which require access to the server) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

301. *See id.* ("The truth, though, is that usually when you're hacked, there's no obvious sign. Hackers work hard to ensure their victims are unaware of what has happened until it's too late, if ever.").

302. *See* Kraft Kennedy, *TeraCopy Forensics: Finding the Elusive "Copy Log"*, KRAFT KENNEDY (April 25, 2017), https://www.kraftkennedy.com/teracopy-forensics-finding-elusive-copy-log/ (indicating that evidence of copying files from a server can disappear quickly) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

303. *Cf.* Orr v. Orr, 440 U.S. 268, 271–72 (1979) (addressing preliminary questions of standing before addressing the merits of the case, even though neither party challenged standing).

304. *Cf. id.* (same).

305. *See* Galaria v. Nationwide Mutual Ins. Co., 663 Fed. App'x 384, 388 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for . . . fraudulent purposes."); *see also* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach."); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) ("[A] substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

hackers will use the victims' data for . . . fraudulent purposes."[306] The Seventh Circuit similarly stated in *Remijas*, "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach."[307] The Ninth Circuit also ruled similarly in *Krottner*, "Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."[308] Lastly, in *Attias*, the D.C. Circuit also agreed, saying, "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."[309]

Courts should conclude that when there is a major hack of an enterprise, there is a presumption that the hacker not only stole the accessed data, but also plans to misuse it.[310] This could, of course, be rebutted by the defendant enterprises, but the burden should be on them.[311] They alone possess the information capable to do this.[312] This presumption would grant standing in data breach cases—unless the defendant rebuts this presumption—by satisfying the U.S. Supreme Court's tests regarding risk of future injury.[313] There is no attenuated chain of possible future actions by a third party that would cause actual injury; there is a very real and almost inevitable chance that someone will have her identity stolen due to the data breach.[314]

---

306. *Galaria*, 663 F. App'x 3d. at 388.

307. *Remijas*, 794 F.3d at 693.

308. *Krottner*, 628 F.3d at 1143.

309. *Attias*, 865 F.3d at 629.

310. *See supra* notes 241–86 (indicating that courts should presume that hackers have ill intent when they hack an enterprise database).

311. *See id.* (same).

312. *See How Do I Know if My Server has Been Hacked,* SERVERPRONTO, *supra* note 302 (listing the ways that someone can tell if her server has been hacked, all of which require access to the server).

313. *Cf. supra* notes 241–86 (indicating that courts should presume that hackers have ill intent when they hack an enterprise database).

314. *Cf. id.* (same).

B. Courts Should Focus on the Actual Hacking Event to Determine Injury, Rather than If the Future Injury has Occurred

In the Non-Standing Cases, the Circuit Courts focus on whether there has been an actual identity theft at the time of the suit.[315] The Third Circuit explicitly states this, saying, "[i]n data breach cases where no misuse is alleged . . . there has been no injury."[316] The Fourth and Eighth Circuits similarly ruled.[317] These courts are not focusing on the correct injury. There are two reasons why: (1) The issue at hand is not whether the plaintiffs' identity was stolen, but that plaintiffs' data was stolen from the defendant entities; and (2) focusing on the question of whether a plaintiff's identity has been stolen creates a circular logic loop out of which plaintiffs could never break. In the Standing Cases, the circuit courts all came to this conclusion.[318]

Courts generally only worry themselves with the two parties before them.[319] With that logic, courts will only focus on the actions of the parties before them in adjudicating any dispute.[320] Yet, in

---

315. *See* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) ("[P]laintiffs make no such claims [of misuse]. This in turn renders their contention of an enhanced risk of future identity theft too speculative."); *see also In re* SuperValu, Inc., 870 F.3d 763, 769–71 (8th Cir. 2017) (focusing on whether future identity theft has occurred); Reilly v. Ceridian, 664 F.3d 38, 44 (3d Cir. 2011) ("Appellants have alleged no misuse, and therefore, no injury.").

316. *Reilly*, 664 F.3d at 45.

317. *See Beck*, 848 F.3d at 274 (explaining that Plaintiffs make no claims of misuse or certainly impending misuse of Plaintiffs' personal information, defeating plaintiffs' standing); *see also In re SuperValu, Inc.*, 870 F.3d at 769–71 (focusing on whether future identity theft as occurred).

318. *See* Galaria v. Nationwide Mutual Ins. Co., 663 F. App'x 384, 391 (6th Cir. 2016) (finding that Plaintiffs have standing to sue when focusing on the hacking injury); *see also* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach."); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data."); Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017) ("No long sequence of uncertain contingencies . . . has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.").

319. *Cf., e.g.*, Gordon v. Biden, 606 F. Supp. 2d 11, 14 (D.D.C. 2009) (dismissing a case because the injury was attributable to third-party actions which were not before the court).

320. *Cf. id.* (same).

these types of cases, the Non-Standing Cases required the hackers to have acted in a particular way at the time of the litigation for there to be sufficient injury to grant standing.[321] This goes against the logic that courts generally follow and against the adversarial process.[322] Courts should, instead, focus on actions that defendants took or did not take that put plaintiffs in the position they sit.

Turning to the second reason, as mentioned several times in this note, there are three requirements for standing: Injury-in-fact, causation, and redressability.[323] While the bulk of this note has focused on the injury aspect of the tripartite standing scheme, if courts analyze the injury in these types of cases to only exist if their identity had been stolen at the outset of litigation, the question then becomes: Did the defendant entity cause the identity theft? While the Supreme Court has implied that the causation element of standing is not as strict as needed to create liability in tort, it is still a necessary element of standing.[324] If the harmed individuals must wait until they are hurt before being able to sue, it becomes an almost insurmountable burden to plead and later prove the causation element.[325] The Seventh Circuit in *Remijas* noted this exact problem:

> Requiring the plaintiffs "to wait for the threatened harm to materialize in order to sue" would create a different problem: "[T]he more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to

321. *See* cases cited *supra* note 315 and accompanying text (listing how the Non-Standing Cases' courts focused on whether the plaintiffs' identities had been stolen).

322. *Cf. Gordon*, 606 F. Supp. 2d at 14 (dismissing a case because the injury was attributable to third-party actions which were not before the court).

323. *See* Lujan v. Def. of Wildlife, 504 U.S. 555, 560–61 (1992) ("First, the plaintiff must have suffered an 'injury in fact' . . . . Second, there must be a causal connection between the injury and the conduct complained of . . . . Third, it must be likely, as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.").

324. *Cf.* Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 125–26, 134 (finding that the causation element of standing was satisfied, but defendant's actions may not have proximately caused plaintiff's injuries).

325. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (indicating that forcing plaintiffs to wait until they are truly harmed would create an almost insurmountable burden for plaintiffs).

> argue that the identity theft is not 'fairly traceable' to the defendant's data breach."[326]

Consequently, if courts force plaintiffs to wait until the future injury occurs, the causation element of standing becomes more tenuous.[327] However, if courts were to focus on the actual hack instead, the Non-Standing Cases' courts would rule that there is no injury.[328] Either way, the plaintiffs would not have standing. This circular logic would continue to go around and around, leaving injured plaintiffs without redress. The only way to escape the loop is to focus on the data breach and conclude—like the circuit courts which decided the Standing Cases did—that the significantly increased chance of future injury is sufficient injury to satisfy constitutional standing.[329]

Reiterating this logic, the Government Accountability Office issued a report that stated, "stolen data may be held 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."[330] This precisely illuminates the danger of waiting for the actual future injury to occur: If the plaintiffs must wait for the damage, they could be waiting for years.[331] As the Seventh Circuit notes, "'the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not "fairly traceable" to the defendant's data breach.'"[332] Ultimately, courts analyzing this issue should focus on the hacking

---

326. *Id.* at 693 (quoting *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n. 5 (N.D. Cal. Sept. 4, 2014)).

327. *See id.* (noting the difficulty in proving causation if the court waits until the hack occurs).

328. *Cf.* cases cited *supra* notes 319–27 and accompanying text (discussing the Non-Standing Case courts' focus on whether there has been an actual identity theft at the time of the suit).

329. *See* cases cited *supra* notes 305–109 and accompanying text (highlighting the Standing Cases courts' presuming that the hacker has ill intent due to the nature of the hack).

330. U.S. GOV'T ACCOUNTABILITY OFF. GAO-07-737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION 29 (2007).

331. *See id.* (describing how long it could take after a data breach for someone's identity to be taken).

332. Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (quoting *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1215 n. 5 (N.D. Cal. Sept. 4, 2014))).

event itself in determining where there is standing, not by what the hackers have done with the data at that point.

C. Conclusion

The courts should presume that a hacker not only accessed compromised information, but also stole and plans to misuse that information. While the defendant could always rebut the presumption with evidence to the contrary, putting the procedural burden upon plaintiffs makes it nearly impossible for plaintiffs to get through the doors of the courthouse.[333] This leaves the injured individuals, whose information is exposed, without redress.[334]

The courts should also not require plaintiffs to sit and wait for the third-party hacker to actually steal identities before plaintiffs can enter the courtroom.[335] Otherwise, courts would in essence be ruling that defendants could not be liable until a third-party acts; a conclusion that is contrary to the American legal system.[336] Such a conclusion would also create circular logic: There could not be standing due to lack of injury until the third-party acts[337]; however, if the third-party hackers do act, it would make the causation element of standing difficult to prove at best.[338] These requirements the Non-Standing Cases' courts have erected cannot be correct. Instead, courts that analyze this issue should not pay attention to whether identity theft has yet occurred but should use the presumption explained above: The hack itself indicates a sufficient risk of future injury to constitute standing.

---

333. *See supra* notes 241–86 (indicating that courts should presume that hackers have ill intent when they hack an enterprise database).

334. *Cf. id.* (same).

335. *See supra* notes 323–32 and accompanying text (arguing that the hacking event is sufficient, and plaintiffs should not be forced to sit and wait for the injury to materialize).

336. *Cf. id.* (same).

337. *See id.* (same).

338. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (indicating that forcing plaintiffs to wait until they are truly harmed would create an almost insurmountable burden for plaintiffs).

IV. Alternatives to Satisfy the Injury-in-Fact Requirement

A. Breach of Privacy

Common law has long protected a person's right to privacy, but the lines have not been clearly delineated.[339] The Second Restatement of Torts [hereinafter "Restatement"] attempted to clear up this ambiguity by stating that the "right of privacy has been defined as the right to be let alone."[340] Furthermore, the Restatement made four separate causes of action that revolved around this theoretical "right to privacy": Intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in a false light.[341]

Of the ones listed above, the most applicable cause of action for these types of data breach cases is an intrusion upon seclusion.[342] The Restatement states, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[343] It is important to note that the comments clearly explain that this "invasion" does not need to be physical, but can be done by using someone's senses, with or without a mechanical aid.[344] This cause of action also does not turn upon whether there was publicity given to the stolen material.[345]

---

339. *See* RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (AM. LAW INST. 1977) (explaining the history of a common law right to privacy).

340. *Id.*

341. *See id.* at § 652A ("The right of privacy is invaded by unreasonable intrusion upon the seclusion of another . . . or . . . appropriation of the other's name or likeness . . . unreasonable publicity given to the other's private life . . . or . . . publicity that unreasonably places the other in a false light before the public.").

342. *Cf. id.* at § 652B (defining an intrusion into seclusion as an invasion into private affairs, such as stealing personal information).

343. *Id.*

344. *See id.* at § 652B cmt. b ("The invasion may be by physical intrusion . . . . It may also be by the use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs.").

345. *See id.* at § 652B cmt. a ("The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs.").

Following this logic and applying those legal principles, if you, hypothetically, were to have your bank account information—which was written on a piece of paper and stored within a safe in your house—stolen, but the paper left in the safe, you have a cause of action for intrusion into seclusion.[346] Beyond that, you would have sufficient injury to pursue a claim against the safe manufacturer if the safe was defective and allowed the criminal to steal your bank account number.[347] However, when that same exact information is stolen from a bank's servers, the Non-Standing Cases' courts would say that you have no standing to sue the bank that may have negligently allowed the hacker to take the information.[348] This is illogical and should not remain. While the exact contours of this "right to privacy" still need to be examined, the current body of law should at least recognize standing in these data breach cases.

B. Personal Data Should Be Recognized Property

The Fourth Amendment protects people from unreasonable searches and seizures.[349] The U.S. Supreme Court has said that these protections extend to personal information, such as GPS locations.[350] However, the Fourth Amendment does not specifically state any protection for personal information. Instead, it lists persons, houses, paper, and effects.[351] Nevertheless, courts have

346. *Cf. id.* at § 652B (listing the elements for intrusion into seclusion cause of action).

347. *Cf.* Redman v. Sentry Group, Inc., 907 F. Supp. 180, 185 (W.D. Va. 1995) *rev'd on other grounds*, Redman v. John D. Brush & Co., 111 F.3d 1174 (4th Cir. 1997) (allowing the plaintiff to sue the safe manufacturer when the plaintiff's safe was defectively made, allowing a thief to steal coins inside).

348. *Cf.* cases cited *supra* note 77 (listing the Non-Standing Cases and the reasons why those courts failed to find standing).

349. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . .").

350. *See* United States v. Jones, 565 U.S. 400, 404 (2012) ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

351. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause.").

still interpreted this list to include personal information.[352] The only logical way to resolve this incongruency is to conclude that personal information is a type of property protected under the Fourth amendment. However, in the context of these data breach cases, the Non-Standing Cases abandon the concept that personal information is a type of private property.[353] If they had not abandoned this concept, the courts would have found there to be sufficient injury to grant standing under a bailor-bailee theory.[354] Furthermore, there would be no need for any risk of future injury analysis; the initial hack is proof enough of injury.[355] Again, while the exact contours of this property right still need to be delineated, the current body of law should at least recognize standing under a property right theory.

V. Conclusion

The circuit split that has emerged causes ambiguity and prevents injured plaintiffs from achieving relief.[356] The current standing requirements that the Non-Standing Cases impose upon plaintiffs present nearly insurmountable burdens.[357] It is time for courts to rule like the Standing Cases.[358] First, courts should presume, for standing purposes, that when a hacker perpetuates a hack upon an enterprise and accesses a confidential database, the

352. *See, e.g.*, *Jones*, 565 U.S. at 404 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

353. *Cf.* cases cited *supra* note 77 (listing the Non-Standing Cases and the reasons why those courts failed to find standing).

354. *Cf., e.g.*, Cont'l Nat'l Am. Grp. v. Valley Line Co., 420 F. Supp. 568, 570 (implying that there was standing to sue because there was a bailor-bailee relationship).

355. *Cf. id.* (implying that there was standing to sue because there was a bailor-bailee relationship).

356. *See* cases cited *supra* note 43 and accompanying text (listing the circuit split regarding data breach cases).

357. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) (indicating that forcing plaintiffs to wait until they are truly harmed would create an almost insurmountable burden for plaintiffs); *see also* cases cited *supra* note 77 (listing the Non-Standing Cases and the reasons why those courts failed to find standing).

358. *See* cases cited *supra* note 77 (explaining why the Standing Cases' courts ruled as they did).

hacker copied the information and plans to misuse it.[359] Second, courts should only focus upon the hacking event when determining if there is injury, not upon whether the hacker, a third-party to the litigation, has yet effectuated an identity theft.[360] The hack alone, because of the presumption listed above, should provide a sufficient risk of future injury to satisfy the Supreme Court's standing jurisprudence.[361] In the alternative, courts should start to recognize that the harmed individuals have standing to sue the hacked enterprise because these types of data breaches violate the common law of intrusion into seclusion.[362] Further, courts should begin to recognize that an individual's private information is that individual's property.[363] Such a conclusion would allow the courts to avoid these difficult future injury inquiries and always find standing for the affected individuals.[364] Regardless of the route that the courts decide to take, plaintiffs, whose personal information was exposed, deserve, at the very least, to get through the court's doors.

---

359. *See supra* notes 241–86 and accompanying text (indicating that courts should presume that hackers have ill intent when they hack an enterprise database).

360. *See supra* notes 319–32 and accompanying text (arguing that the hacking event is sufficient to grant standing and plaintiffs should not be forced to sit and wait for the injury to materialize).

361. *Compare id.* (arguing that the hacking event is sufficient and plaintiffs should not be forced to sit and wait for the injury to materialize), *and supra* notes 241–88 and accompanying text (indicating that courts should simply presume that hackers have ill intent when they hack an enterprise database), *with* cases cited *supra* notes 45–75 (explaining the current constitutional standing jurisprudence).

362. *See supra* notes 341–48 and accompanying text (arguing that courts should recognize that an individual has standing to sue the hacked enterprise through an intrusion into seclusion cause of action).

363. *See supra* notes 351–58 and accompanying text (arguing that courts should recognize that an individual's personal information is property).

364. *Cf., e.g.*, Continental Nat'l Am. Group v. Valley Line Co., 420 F. Supp. 568, 570 (implying that there was standing to sue because there was a bailor-bailee relationship).