University of Cincinnati Law Review

Volume 88 | Issue 4 Article 9

May 2020

The Time Between the Theft and the Injury: Standing Requirements Based on a Future Risk of Identity Theft After a Data Breach

Jameson Steffel
University of Cincinnati, steffejn@mail.uc.edu

THE TIME BETWEEN THE THEFT AND THE INJURY: STANDING REQUIREMENTS BASED ON A FUTURE RISK OF IDENTITY THEFT AFTER A DATA BREACH

Jameson Steffel

I. INTRODUCTION

A single data breach has the ability to affect billions of accounts at one time.[1] In 2018 alone, data breaches exposed over 446 million consumer records containing personally identifiable information ("PII").[2] Although the numbers may already seem staggering, some believe the risk will likely increase and worsen going forward as reliance on online record keeping increases.[3] Unsurprisingly, as data breaches occur, victims bring lawsuits, hoping to remedy damages. Corporate spending on class action lawsuits has increased to its highest level since 2008.[4] Within the trend, many in the field believe data privacy and security will bring the next wave of class action suits.[5]

As the legal attention surrounding data and security has increased, federal courts are split on when a victim of a data breach has standing to sue in federal court. Federal courts generally agree that someone whose identity was stolen and wrongfully used after their PII was exposed in a data breach has standing to sue.[6] However, federal courts are split over whether risk of future identity theft alone is enough to grant standing in

1. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affect by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html?module=inline.

2. IDENTITY THEFT RES. CTR., 2018 END-OF-YEAR DATA BREACH REPORT 2 (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf [https://perma.cc/AMA7-PC8E].

3. Brue Schneier, Opinion, *Internet Hacking Is About to Get Much Worse*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/opinion/internet-hacking-cybersecurity-iot.html.

4. CARLTON FIELDS, 2019 CARLTON FIELDS CLASS ACTION SURVEY: BEST PRACTICES IN REDUCING COST AND MANAGING RISK IN CLASS ACTION LITIGATION 7 (2019), https://gallery.mailchimp.com/0c82d1e732eec64ff4cb3d4b7/files/d46d1d29-390d-48ec-ac98-50c7e8600edc/2019_Class_Action_Survey.pdf [https://perma.cc/927U-P55R].

5. *Id.* at 13 ("More than half of legal decision-makers responsible for class actions believe data privacy and security will be the next wave of class actions, up from less than 30 percent in 2017.").

6. *See* Stevens v. Zappos.com, Inc. (*In re* Zappos.com, Inc., Customer Data Sec. Breach Litig.), 884 F.3d 893, 895 (9th Cir. 2018) (District court separated the plaintiffs into two classes: plaintiffs who "alleged that they had already suffered financial losses from identity theft" and those who had not already suffered damages. On appeal, parties only contested whether the second group of plaintiffs lacked standing. The Ninth Circuit seemed to agree there were not questions regarding standing for the first group of plaintiffs); *See also*, Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017) ("Nobody doubts that identity theft, should it befall one of these plaintiffs, would constitute a[n] . . . injury.").

federal courts.[7]

This Article explores the aforementioned split and focuses on how two recent cases have interpreted previous decisions on either side of the split. Further, based on the recent rulings, this Article argues that the split may be harmonized. Part II of this Article first sets forth the framework of the standing doctrine. Next, Part II discusses two Supreme Court decisions, *Clapper v. Amnesty Int'l USA*[8] and *Spokeo, Inc. v. Robins*,[9] that relate directly to the standing doctrine and the current circuit split, along with other background cases necessary for fully understanding the circuit split. Part III compares two recent cases involved in the circuit split: *Beck v. Mcdonald*[10] and *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*.[11] Part IV argues that although *Beck* and *AFGE* fall on opposite sides of the circuit split, together the cases illustrate that federal courts have generally come to agreement on what factors are the most important when deciding whether to grant standing for plaintiffs alleging risk of future identity theft. Further, Part IV also proposes a framework for courts to use that harmonizes the holdings of these different cases. Finally, Part V concludes by summarizing the above issues and advocating that, moving forward, courts should follow the simplified framework suggested.

II. BACKGROUND

This Part first introduces the standing doctrine and then introduces the two major Supreme Court cases from the last decade, *Clapper* and *Spokeo*, which provide guidance to lower courts for determining if plaintiffs have standing in data breach cases. Although neither case's facts dealt specifically with a data breach, both cases discussed standing and sought to clarify how courts should determine if a plaintiff had suffered an injury in fact.

A. The Standing Doctrine

Article III of the United States Constitution grants federal courts with "[t]he judicial Powers of the United States,"[12] but limits the power to only

7. AFGE V. OPM (*In re* United States OPM Data Sec. Breach Litig.), 928 F.3d 42, 58 (D.C. Cir. 2019).

8. 568 U.S. 398 (2013).

9. 136 S. Ct. 1540 (2016).

10. 848 F.3d 262 (4th Cir. 2017).

11. 928 F.3d 42 (D.C. Cir. 2019).

12. U.S. CONST. art. III §1.

"Cases" and "Controversies."[13] "Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy."[14] The idea behind a standing requirement is to "prevent the judicial process from being used to usurp the powers of the [other] political branches."[15] Therefore, plaintiffs must establish the "irreducible constitutional minimum" of standing's three elements.[16]

To establish standing, a plaintiff must show (1) the plaintiff suffered an injury in fact, (2) the injury is fairly traceable to the challenged conduct of the defendant, and (3) that the injury is likely to be redressed with a favorable judicial ruling.[17] The first element, injury in fact, must be "(a) concrete and particularized and (b) actual or imminent, not 'conjectural' or 'hypothetical.'"[18] Many times, the first standing element is the prominent issue in data breach suits.[19] Lastly, the plaintiff "bears the burden of establishing standing" when it invokes federal jurisdiction.[20] Meeting the burden on all three elements of standing allows the case to be heard before the court.

B. Clapper v. Amnesty International[21]

Clapper dealt with a facial constitutional challenge to a new amendment to the Foreign Intelligence Surveillance Act of 1978 ("FISA").[22] More specifically, the plaintiffs sought to declare FISA §1881a unconstitutional[23]. Essentially, FISA §1881a allowed the government to more easily authorize foreign intelligence surveillance without the traditional requirements of probable cause and similar constraints.[24] The plaintiffs were comprised of "organizations whose work allegedly require[d] them to engage in sensitive and sometimes privileged" communications with individuals who they believed to be

13. U.S. CONST. art. III §2.
14. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
15. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).
16. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).
17. *Id.* at 560, 561.
18. *Id.*
19. *See Infra*. Parts II, III.
20. *Clapper*, 568 U.S. at 412.
21. 568 U.S. 398 (2013).
22. *Id.* at 407.
23. *Id*. at 404.
24. *Id*. at 405. ("Amendment Act . . . creat[es] a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-US persons located abroad. Unlike traditional FISA surveillance, §1881a does not require the Government to demonstrate probable cause that the target [of surveillance] is a foreign power or agent … does not require the Government to specify the nature and location of … surveillance.").

"likely targets of surveillance under [FISA] §1881a."[25] The plaintiffs' two main arguments were (1) "there [was] an objectively reasonable likelihood that their communications [would] be acquired under §1881a at some point in the future, thus causing them injury" and (2) the "risk of surveillance" was "so substantial" the plaintiffs were "forced to take costly and burdensome measures to protect the confidentiality."[26]

Initially, the district court held that the plaintiffs did not have standing.[27] Then, on appeal, the Second Circuit reversed the district court's decision and agreed with the plaintiffs that there was an objectively reasonable likelihood that their communications would be intercepted.[28] The Supreme Court reversed the Second Circuit's finding, siding with the government in a 5-4 decision.[29]

The Court first ruled on the standing doctrine by taking issue with the Second Circuit's belief that "an objectively reasonable likelihood" of future harm was sufficient to establish standing.[30] Instead, the Court reiterated that the "well-established requirement"[31] for standing when dealing with a future threated injury was that the injury must be "certainly impending."[32] An objectively reasonable likelihood was considered too low of a bar for standing.[33]

Further, the Court continued that the premise of the plaintiffs' argument rested on "a highly attenuated chain of possibilities" that relied on independent actors making independent choices, of which the plaintiffs could only speculate.[34] This speculative chain of possibilities further prevented the plaintiffs from satisfying the second element of standing (*i.e.*, that an injury in fact was fairly traceable to FISA §1881a).[35]

Lastly, in *Clapper* the Court also found issue with the plaintiffs' alternative argument.[36] The plaintiffs believed they had established standing and an injury in fact because they were forced to suffer costs and burdens in an effort to avoid FISA §1881a surveillance.[37] Instead, the Court clarified that the party bringing the action "cannot manufacture standing merely by inflicting harm on themselves based on their fears of

25. *Id*. at 406.
26. *Id.* at 407.
27. *Id.*
28. *Id.*
29. *Id.* at 422.
30. *Id.* at 410.
31. *Id.* at 401.
32. *Id*. at 410.
33. *Id.*
34. *Id.* at 411, 412.
35. *Id.*
36. *Id.* at 415.
37. *Id.* at 415, 416.

hypothetical future harm."[38] Effectively, the reasoning circles back to whether the threat of injury passes the "certainly impending" test. If it does not, then a plaintiff will not have standing because the injury cannot simply be the costs and burdens incurred to avoid a threat that is not "certainly impending."

Interestingly, in a footnote, the Court noted that its cases "do not uniformly require plaintiffs to demonstrate that [plaintiffs are] literally certain that the harms they identify will come about."[39] Further, the Court stated "[i]n some instances, we have found standing based on a 'substantial risk' that the harm will occur."[40] Later, in *Susan B. Anthony List v. Driehaus*[41] ("*SBA List*"), the Court treated both the "certainly impending" and "substantial risk" test as valid.[42] Moreover, the Court in *SBA List* seemed to rely on the substantial risk test.[43]

Since *SBA List* and *Clapper*, some courts have suggested the more stringent "certainly impending" standard used in *Clapper* should be applied to cases dealing with national security or separation of powers issues, as was the case in *Clapper*.[44] Overall, between the two cases, it is clear that to pass the standing requirements, the Court will use one of the two standards. The substantial risk standard is a lower bar for a plaintiff to satisfy.[45] Still, the facts and circumstances of the individual case will likely determine which standard is used by courts. If the case involves national security or other separation of powers issues, it is more likely that courts will use the more restrictive "certainly impending" standard, but the Court has not specifically clarified this conclusion.

C. Spokeo, Inc. v. Robins[46]

The 2016 Supreme Court decision in *Spokeo* resulted in stricter

38. *Id.* at 416.

39. *Id.* at 410, n.5.

40. *Id.*

41. 573 U.S. 149 (2014).

42. *Id.* at 158.

43. See Bradford C. Mank, *Data Breaches Identity Theft, and Article III Standing: Will the Supreme Court Resolve the Split in the Circuits,* 92 NOTRE DAME L. REV. 1323, 1334 (2017). "In *Susan B. Anthony* the Court treated both tests in *Clapper* as valid . . . [t]he *Susan B. Anthony* decision appeared to rely on the substantial risk test in concluding that 'the threat of future enforcement of the false statement statute [was] substantial.'" *Id.* (citing Susan B. Anthony List v. Driehaus, 573 U.S. 149, 164 (2014)).

44. Stevens v. Zappos.com, Inc. (*In re* Zappos.com, Inc., Customer Data Sec. Breach Litig.), 884 F.3d 893, 897 (9th Cir. 2018) ("*Clapper*'s standing analysis was "especially rigorous" because the case arose in a sensitive national security context.").

45. Mank, *supra* note 43, at 1333 ("[T]he Court had sometimes used a less strict "substantial risk" test.").

46. 136 S. Ct. 1540 (2016).

requirements for the first element of Article III standing: injury in fact.[47] More specifically, *Spokeo* required that a plaintiff allege an injury that was both "concrete *and* particularized."[48]

The issue in *Spokeo* was whether a violation of the Fair Credit Reporting Act ("FCRA") by Spokeo, Inc. ("Spokeo") gave the plaintiff standing in federal court.[49] The FCRA regulates companies that provide information about consumers' credit worthiness and imposes various rules regarding the creation and use of consumer reports.[50] One of those rules is that such agencies must "follow reasonable procedures to assure maximum possible accuracy" of the information they collect and produce.[51] In its analysis, the Court treated Spokeo as a company regulated under the FCRA.[52] The plaintiff discovered that the information Spokeo reported on his report was inaccurate, which constituted a violation under the FCRA.[53]

The district court ruled that the plaintiff did not have standing because he had not pled an injury in fact.[54] The Ninth Circuit then reversed, finding that a "violation of a statutory right [was] usually a sufficient injury in fact to confer standing." The Ninth Circuit further noted that there was standing because the injury was particularized to the plaintiff specifically.[55]

The Supreme Court's analysis focused wholly on the injury in fact requirement of standing. Specifically, the Court focused on what the "particularized" and "concrete" elements of standing require.[56] The Court concluded that the "particularized" element meant the injury must be personal and in an individualized manner, which means the plaintiff has suffered "actual or threatened injury."[57] Importantly for data breach cases, the Court included that a "threatened injury" potentially could satisfy the "particularized" element. However, the Court emphasized that "concrete" and "particularized" are not the same element.[58] Instead, the two elements have different characteristics, and both are required for a plaintiff to have

47. *Id.* at 1545.

48. *Id.*

49. *Id.* at 1544.

50. *Id.* at 1545.

51. *Id.*

52. *Id.* at 1546 ("Spokeo is alleged to qualify as a consumer reporting agency under FCRA.") (internal quotes omitted).

53. *Id.*

54. *Id.*

55. *Id.* ("Spokeo violated *his* statutory rights . . . not just other people[s] . . . because his personal interests in the handling of his credit information are individualized.") (internal quotations omitted).

56. *Id*. at 1548.

57. *Id.*

58. *Id.*

standing.[59]

The Court continued by defining "concrete" injury as one that "must actually exist" and must be "real, and not abstract."[60] The Court also stated, however, that concrete does not necessarily mean tangible, and instead noted that "intangible injuries can nevertheless be concrete."[61] Both history[62] and Congress play a pivotal role in shaping whether an intangible harm creates an injury in fact.[63] Congress may elevate an intangible harm to the status of being a concrete injury by creating statutory law.[64] The result is that an intangible harm becomes a *de facto* injury.[65] Essentially, a statute can create standing for an otherwise intangible harm. However, the Court warned that "a bare procedural violation" without any other harm would not satisfy the injury in fact requirement of standing.[66] Therefore, the Court held that the plaintiff may not satisfy the concreteness element by alleging a bare procedural violation.[67] To illustrate, the Court used the example of an inaccurate zip code.[68] An inaccurately reported zip code would not alone cause harm to a plaintiff, but it still technically would be inaccurate information and therefore violate the statute. Although it is a procedural violation, an inaccurate zip code would not constitute concrete harm. The Court remanded the case and instructed the Ninth Circuit to determine whether other types of false information would be considered a concrete harm.[69]

Altogether, the *Spokeo* decision offers guidance on the standing jurisprudence in data breach cases in a few different ways. First, the injury must be both concrete and particularized. If the individual has personally suffered threatened injury, then the individual will likely satisfy the "particularized" element. For the concrete element, statutory violations help to confer standing for individuals. However, a statutory violation must be more than a mere procedural violation. In dealing with future harm, the Court suggested that a procedural violation must "entail a degree of risk sufficient to meet the concreteness requirement."[70] This

59. *Id.*

60. *Id.* (Internal quotations omitted).

61. *Id.* at 1549.

62. History is simply determining whether the harm has traditionally been considered adequate for standing. "It is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regard as providing a basis for a lawsuit in . . . courts." *Id.* at 1549.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.* at 1550.

68. *Id.*

69. *Id.* at n.8.

70. *Id.* at 1550.

means that the violation itself must at least potentially pose a genuine harm to the person. If not, the plaintiff will likely be held not to have standing.

D. The D.C. Circuit's Prior Decision Considering Clapper *and* Spokeo

Since the Court's decisions in *Clapper* and *Spokeo*, lower federal courts remain split on the issue of whether future risk of identity theft is sufficient to meet the standing requirements of Article III. Before the discussion of the D.C. Circuit's recent 2019 decision in *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*[71] contained in Part III, it is important to understand how the D.C. Circuit decided its first ruling that dealt with a future harm of identity theft after the rulings in *Clapper* and *Spokeo*.

1. Attias v. CareFirst, Inc.[72]

The *Attias* case arose out of a cyberattack against health insurer CareFirst, Inc.[73] In the cyberattack, customers' personal information was breached after CareFirst allegedly failed to encrypt its customer data.[74] The plaintiffs' causes of action included, inter alia, violations of various state statutes, negligence, and breach of contract.[75] The parties disagreed over what the plaintiffs' complaint alleged.[76] Specifically at issue was whether the complaint alleged theft of information that included social security numbers and credit card numbers or merely customer names, addresses, and subscriber ID numbers.[77] The district court read the complaint to not include social security and credit card information.[78] Without these other forms of identifying data, the plaintiffs could not demonstrate how the hackers could steal the plaintiffs' identities.[79] Therefore, the district court ruled that the injury was too speculative.[80] In other words, the district court found the injury in fact was not "actual or imminent" because the hackers could not access these forms of identifying data.[81]

71. 928 F.3d 42 (D.C. Cir. 2019).
72. 865 F.3d 620 (D.C. Cir. 2017).
73. *Id.* at 622.
74. *Id.* at 623.
75. *Id.* at 623. In total the plaintiffs raised eleven different state-law causes of action. *Id.*
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.* at 626.

On appeal, the D.C. Circuit disagreed and reversed the decision of the district court.[82] A few factors went into the court's decision. First, the district court erred by not reading the complaint to include social security numbers and credit card numbers.[83] The complaint alleged the business collected all sorts of customer PII, and the plaintiffs' defined PII to include patient credit cards and social security numbers in the complaint.[84] Therefore, since the court concluded that the complaint did include PII necessary for identity theft, the complaint then also plausibly alleged the breach could potentially expose customer information to identity theft.[85] Secondly, the court believed the facts in the case were quite distinct from *Clapper*, specifically because the plaintiffs' alleged risks were not contingent upon the happenings of a series of possible events.[86] Here, the hacker had already accessed the PII.[87] Further, once the hack occurred, the court said it was far less speculative to infer both the hacker's intent and ability to use the data for ill will.[88] The court noted that "simply by virtue of the hack and the nature of the data . . . taken" a substantial harm existed.[89]

Lastly, the *Attias* court made an important distinction regarding whether a plaintiff's "self-imposed risk-mitigation costs" conferred standing to the plaintiff.[90] After the data breach, the plaintiffs alleged that they reasonably spent money to protect their data by purchasing identity theft protection and monitoring services.[91] Further, the plaintiffs incurred costs from time spent responding to the incident and monitoring their credit and accounts afterwards.[92] By quoting part of the *Clapper* decision, the court concluded that "such self-imposed risk-mitigation costs, when 'incurred in response to a speculative threat,' do not fulfill the injury requirement."[93] However, the court also noted that plaintiffs can use these costs to "satisfy the redressability requirement, when combined with a risk of future harm that is substantial enough to qualify as an injury in

82. *Id.*

83. *Id*. at 627.

84. *Id.*

85. *Id.* at 628.

86. *Id.*

87. *Id.*

88. *Id.* at 628-29. Quoting the seventh circuit, the court noted, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is sooner or later, to make fraudulent charges or assume the consumers' identities." *Id.* (quoting Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015)).

89. *Id.* at 629.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.* (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416-17 (2013)).

fact."[94] In this case, the court agreed with the plaintiffs that spending money to protect against the threat was reasonable.[95] Overall, the court's conclusion suggests that if the first element of standing—injury in fact—is satisfied, then mitigation costs may be used to meet the third element of standing—redressability.

III. THE CIRCUIT SPLIT

Since the two Supreme Court cases discussed in Part II and the D.C. Circuit's initial decision in *Attias*, the split has continued to be a highly contested issue, as discussed more fully in this Section. First, this Section examines the Fourth Circuit's 2017 decision in *Beck v. McDonald*, where the court refused to grant standing for a risk of future identity theft claim.[96] Then, this Section reviews the recent 2019 D.C. Circuit decision in *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*,[97] in which the court granted standing based on a future risk of identity thief.[98] Together, the cases illustrate the current legal landscape of the circuit split by focusing on the similar factors the courts used when deciding when to grant standing to potential future victims of identity theft.

A. Beck v. McDonald

The *Beck* decision dealt with two consolidated cases that arose out of a laptop computer and pathology reports that were either misplaced or stolen from a Veteran Affairs medical center.[99] An internal investigation found that the laptop was "likely stolen" and that the medical center violated its own policies by leaving the client's information stored on the laptop unencrypted.[100] The plaintiffs were veterans who received treatment and healthcare from the VA medical center.[101] The plaintiffs alleged violations of the Privacy Act of 1974 and the Administrative Procedure Act.[102] In response to the investigation, hospital officials notified every patient whose information may have been on the laptop or in the reports and offered a year of free credit monitoring to those possibly affected by the breach.[103] Unsatisfied, the plaintiffs sued and tried to

94. *Id.*
95. *Id.*
96. 848 F.3d 262, 267 (4th Cir. 2017).
97. 928 F.3d 42 (D.C. Cir. 2019).
98. See Section III.B.
99. *Beck*, 848 F.3d at 266.
100. *Id.* at 267.
101. *Id.* at 266.
102. *Id.*
103. *Id.* at 267.

establish standing through (1) their increased risk of future identity theft and (2) the costs they incurred to protect themselves against identity theft.[104]

After discovery, the district court granted the defendant's motion to dismiss, holding that the plaintiffs lacked standing under Article III since they had not "submitted evidence sufficient [to show] they faced a 'certainly impending' risk of identity theft."[105] Citing *Clapper*, the district court agreed that the claims were "too speculative" because they were "contingent on a claim of attenuated hypothetical events."[106] Specifically, the district court said the fact that "33% of those affected by the laptop theft would have their identities stolen" was not enough to demonstrate "a substantial risk of identity theft" or pass the "lesser standard" of "substantial risk."[107] Since the court considered the threat of future identity theft merely speculative, it followed that the court believed that the plaintiffs purchasing credit monitoring services "did not amount to an injury-in-fact because they were taken solely 'to mitigate speculative harm.'"[108]

The Fourth Circuit conducted a *de novo* review of the district court's decision.[109] After review, the Fourth Circuit agreed with the district court and held that the plaintiffs lacked Article III standing.[110] The focus of the court's inquiry was whether the plaintiffs met the first element of Article III standing: injury in fact.[111] The court analyzed two potential theories proposed by the plaintiff for standing: "(1) increased risk of future identity theft and (2) costs of protecting against the same" under both the certainly impending standard and the "substantial risk" standard.[112]

In its analysis of the increased risk of future identity theft under the certainly impending standard, the court specifically discussed the current circuit split.[113] In the court's opinion, the facts of *Beck* were distinguishable from the cases of other circuits that granted standing based on future risk of identity theft because those cases had "common allegations that sufficed to push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent."[114] As an

104. *Id.* at 266-67.

105. *Id.* at 268.

106. *Id.* (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013)).

107. *Id.*

108. *Id.*

109. *Id.* at 269.

110. *Id.* at 267.

111. *Id.* at 270.

112. *Id.* at 273.

113. *Id.* (noting the Sixth, Seventh, and Ninth Circuits granting standing and the First and Third Circuits denying standing).

114. *Id.* at 274.

example, the court noted that in *Galaria*,[115] *Remijas*,[116] and *Pisciotta*,[117] the hackers intentionally targeted the personal information that was stolen in the data breach and at least one of the named plaintiffs had alleged actual "misuse or access" to the personal information by the thief.[118] In *Beck* no such claims were made.[119]

In reaching its holding, the court stated (1) there was no evidence that the PII stored on the laptop had been accessed and (2) the significant amount of time that passed since the incident made the risk more speculative.[120] The court accepted the allegation that the laptop was stolen, but said "the mere theft of [the laptop], without more, cannot confer Article III standing."[121] Without more, the Fourth Circuit could not "assume that the thief targeted the stolen items for the personal information they contained."[122] Overall, it was clear the Fourth Circuit was reluctant to grant the plaintiffs standing without more evidence that illustrated the thief intended to misuse the stolen PII.

The court also held that the plaintiffs fell short of the burden under the "substantial risk" standard.[123] The plaintiffs alleged they faced a substantial risk of future identity theft for three reasons: (1) a third of all health-related data breaches resulted in identity theft; (2) the defendants already spent millions to mitigate the future risk; and (3) the defendants "effectively conceded" that the theft constituted a "reasonable risk" because they offered plaintiffs free credit monitoring for a year.[124] In its "substantial risk" analysis, the court stated that statistics were insufficient to establish a substantial risk of harm.[125] Further, in a footnote, the court demonstrated a reluctance to use general statistics because statistics are not particularized to the case at issue.[126] The court also declined "to infer a substantial risk . . . from an organization's offer to provide free credit monitoring services,"[127] even though other courts had come to the opposite conclusion.[128] Lastly, the court read *Clapper* to reject a

115. Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 388 (6th Cir. 2016).

116. Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693, 694 (7th Cir. 2015).

117. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2015).

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

119. *Id.*

120. *Id.* at 274-75.

121. *Id.* at 275.

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.* at 276.

126. *Id.* at 275-76, n.7 ("This general statistic says nothing about the risk arising out of any particular incident, nor does it address the particular facts of this case").

127. *Id.* at 276.

128. *Id.* Footnote 8 of *Beck* acknowledges *Galaria* and *Remijas* came to the opposite conclusion. *Id*., n.8.

"reasonable risk" as being sufficient to meet the imminent requirement of an injury in fact.[129]

In the final part of its analysis, the court discussed whether costs of mitigative measures incurred by plaintiffs could, by itself, confer standing.[130] The court highlighted the circularity that plagues the reasoning to confer standing for this sole purpose, describing the claim as merely "a repackaged version" of the substantial risk analysis.[131] Essentially, the costs to mitigate the risks of future identity theft could confer standing only if there was a substantial risk of the identity theft occurring in the future. Therefore, costs of mitigating future damages, by itself, "simply put … cannot confer standing."[132] In many ways, the court's reasoning echoed the *Spokeo* decision that came to the same conclusion.

B. AFGE v. OPM (In re United States OPM Data sec. Breach Litig.)[133]

In June 2019, the D.C. Circuit again ruled on the circuit split. This time, the case concerned a government agency data breach by hackers.[134] The data stolen included many types of sensitive information, such as birthdates, social security numbers, and fingerprints.[135] In total, the breach affected over twenty-one million people.[136]

The agency at issue was the U.S. Office of Personnel Management ("OPM"), which is the federal government's chief human resources agency and maintains the electronic personnel files of federal employees and job applicants.[137] Using stolen credentials from a third-party company that helped the agency with its background checks, cyberattackers hacked the network multiple times from 2013 to 2014.[138] The cyberattacks were described as "sophisticated, malicious, and carried out to obtain sensitive information for improper use."[139] The OPM had experienced cyberattacks since 2009 and had been warned of serious deficiencies in their security

129. *Id.*

130. *Id.*

131. *Id.*

132. *Id.* at 276, 277 (quoting Remijas v. Neiman Marcus Grp, LLC, 794 F.3d 688, 694 (2015)).

133. 928 F. 3d 42 (D.C. Cir. 2019).

134. *Id.* at 49.

135. *Id.* at 49-50. Other information included criminal histories, physiological and emotional health, finances, residency details and passport information. It also included information about spouses and cohabitants. *Id*.

136. *Id.* at 49.

137. *Id.*

138. *Id.* at 50.

139. *Id.* at 52.

systems as far back as 2007.[140] After announcing the breaches in 2015, OPM offered fraud monitoring, identity theft protection services, and insurance to those affected by the breach at no costs for either eighteen months or three years.[141]

Despite the OPM's offer, multiple suits arose across the country and were consolidated into two complaints against OPM.[142] One complaint was brought by the American Federation of Government Employees ("Arnold plaintiffs") and second complaint was brought by three members of the National Treasury Employees Union ("NTEU").[143] Arnold plaintiffs sought damages from OPM under Section 552a(e)(10) of the Privacy Act of 1974, while NTEU sought declaratory and injunctive relief and claimed a violation of their "constitutional right to information privacy."[144]

The district court dismissed both complaints for lack of standing.[145] First, the district court did not believe a "risk of future identity theft was either substantial or clearly impending" unless the plaintiffs experienced "out-of-pocket losses" from the "actual misuse of their data."[146] Secondly, even the plaintiffs who had their data actually misused lacked standing because the misuse was not tracible to the OPM's data breaches particularly.[147]

On appeal, the D.C. Circuit held that both sets of plaintiffs "cleared the low bar to establish their standing at the pleading stage."[148] The NTEU plaintiffs claimed a constitutional right to "information privacy."[149] When determining whether a plaintiff has standing, the court "must assume *arguendo*, the merits of his or her legal claim."[150] Therefore, the court assumed the NTEU plaintiffs had a right to information privacy. The court thought this right was violated when the cyberattackers stole the personal information of the plaintiffs.[151] In its short analysis, the court concluded

140. *Id.* at 51. Further, in 2014 the Inspector General advised the agency to shut down the operating system due to existing security vulnerabilities. *Id*.

141. *Id.* at 50. (stating the time of free services depended on whether the specific individual's social security number had been compromised in the data breach.).

142. *Id.*

143. *Id.*

144. *Id.* at 50-52. Arnold plaintiffs also brought claims against KeyPoint, the third-party company OPM used to conduct a majority of its background and security clearance, but this Article will not discuss those claims. *Id*. at 50-51.

145. *Id.* at 53.

146. *Id.* at 53.

147. *Id.* Essentially, there were possible alternatives beyond the OPM data breach that could have led to the subsequent misuse of the plaintiffs' data. *Id*.

148. *Id.* at 61 (quoting Attias v. Carefirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017)).

149. *Id.* at 53.

150. *Id*. at 54 (citing Estate of Boyland v. Department of Agric., 913 F.3d 117, 123 (D.C. Cir 2019)).

151. *Id.*

the nature of the constitutional claim granted standing to the NTEU plaintiffs.[152] On the other hand, the Arnold plaintiffs' analysis was much more involved. The opinion broke down its analysis by discussing each of the three elements of standing.[153] This Article's analysis follows the same format.

1. Injury in Fact

The D.C. Circuit's analysis started by citing *Attias* as a reminder that the risk of future identity theft was already recognized as a "concrete and particularized injury."[154] However, based on *Clapper* and *SBA List*, the injury must also be clearly impending or substantial.[155] The court compared the current case to *Attias*.[156] In comparing the two cases, the D.C. Circuit focused on two factors in particular: "both the intent and the ability to use the data for ill (will)."[157] The court concluded that in both cases, the intent of the hacker and the nature of the data stolen made the risk of future identity theft a substantial risk.[158]

The court reasoned that the ability to use data for ill will essentially turned on the type of data that a hacker collected in its breach.[159] After the data breach, hackers had "in their possession all information needed to steal the Arnold plaintiffs' identities."[160] Based on the information taken, "[i]t hardly [took] a criminal mastermind to imagine how such information could be used to commit identity theft."[161] The Arnold plaintiffs' claims that some members already experienced forms of identity theft further bolstered the plaintiffs' inference that the nature of the data stolen contained sufficient information to successfully steal someone's identity.[162] Overall, combining the fact that the plaintiffs had already suffered identity fraud with the "obvious potential" for future fraud based on "the information stolen during the breaches" moved the risk of future identity theft from speculative to substantial.[163]

The court's intent analysis was premised on the Seventh Circuit's

152. *Id.* at 55.

153. *See supra* Section II(A).

154. *AFGE*, 928 F.3d at 55.

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

156. *Id.* at 55-58.

157. *Id.* at 56.

158. *Id.* at 58.

159. *Id.*

160. *Id.* at 56.

161. *Id.*

162. *Id.* ("several Arnold Plaintiffs also allege that unauthorized charges have appeared on their existing credit card and bank account statements since the breaches.").

163. *Id.* at 58.

Remijas[164] opinion, which determined that when a hacker breaks into a database and steals private consumer information, the purpose "is, sooner or later, to make fraudulent charges or assume those consumers' identities."[165] The OPM argued that its case was different since (1) the attack was against the United States government and (2) the hackers had others goals which explained why the hackers wished to obtain the PII, such as national security and espionage objectives.[166] The court found two problems with the OPM's theories. First, the theories were based on the district courts' "own extra-record research" which was not allowed.[167] Secondly, "espionage and identity theft [were] not mutually exclusive."[168] The court noted that, at the pleading stage, it was not appropriate to sort out the most likely explanation for the hacker's objective.[169] Lastly, the court explained that in scenarios like the current case, where the plaintiff's identity was already alleged to have been stolen, the importance of proving the hackers intent "becomes markedly less important" because possible damage from the breach had already manifested.[170]

The court used hacker intent and subsequent misuse of stolen information to distinguish *AFGE* from the Third and Fourth Circuit decisions that did not grant standing due to future risk of identity theft.[171] In both of these cases that denied standing, the court concluded that (1) neither plaintiff alleged the theft intentionally accessed the private information and (2) there were no events of identity theft after the hack.[172] In *AFGE*, the court said the plaintiff alleged both the hacker's intention and subsequent misuse.[173]

Lastly, the court's analysis of *Beck* forced the court to consider whether the time that elapsed since the breach should be considered as a factor, along with intent and the nature of the data stolen. It agreed with *Beck* that "as a general principle … as breaches fade further into the past, threatened injuries become more and more speculative."[174] The dissent believed that a gap of around two years between the attack and the

164. 794 F. 3d 688, 690 (7th Cir. 2015). *Remijas* was also a data breach case where the Seventh Circuit granted standing to the plaintiffs based on a future risk of identity theft. In *Remijas*, hackers attacked the department store Neiman Marcus Group and stole customer data. Approximately 350,000 cards were exposed to the hacker's malware. *Id*. at 689-690.

165. *AFGE*, 928 F.3d at 56 (quoting *Remijas* 794 F.3d at 693).

166. *Id.* at 57.

167. *Id.*

168. *Id.*

169. *Id.*

170. *Id.* at 58.

171. *Id.* at 58-59.

172. *Id.* at 58.

173. *Id.*

174. *Id.* at 59.

subsequent misuse of the data was enough to "render the threat of future harm insubstantial."[175] The majority, however, was not willing to explicitly rule on the timing issue because (1) such "massive scale" data breaches were a "relatively new phenomenon" and (2) the type of information stolen was particularly sensitive.[176] Overall, "notwithstanding the passage of time and the governmental character of the databases at issue," the Arnold plaintiffs still offered enough evidence, at least at this stage in the proceeding, to demonstrate a substantial risk of future identity theft.[177]

2. Causation

The D.C. Circuit overruled the district court's finding that the Arnold plaintiffs did not meet the causation element of standing.[178] Instead, the court had "little difficulty concluding" that the plaintiffs met their "relatively modest burden" of alleging traceability to the OPM data breach.[179] Initially, the district court said the plaintiffs did not allege "any facts that plausibly connect" the misuse of the stolen data to the breaches of the OPM systems.[180] However, the circuit court clarified that the district court used the wrong premise. For future risk of identity theft injury claims, instead of focusing on past attacks, the question is whether the injury is fairly traceable to the risk of *future* identity theft.[181] Here, the data had been stolen, and the OPM had failed to secure its information systems, despite repeated warnings by the General Inspector.[182] Further, the data stolen was enough by itself to enable several forms of identity theft.[183] Together, the court found all of these reasons sufficient to meet the causation burden for standing by holding that the a future risk of identity theft was traceable to the OPM.[184]

3. Redressability

The D.C. Circuit held that the plaintiffs could satisfy the redressability element by receiving compensation for their related mitigation expenses,

175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.* at 60.
179. *Id.* at 61.
180. *Id.* at 60.
181. *Id.* at 59-60.
182. *Id.* at 60.
183. *Id.*
184. *Id.* at 61.

if the plaintiff were to prevail on their claim.[185] In *AFGE*, the related mitigation expenses were the costs the plaintiffs incurred to monitor their credit.[186] The court cited *Attias* and used its logic that plaintiffs may be redressed for their monetary costs spent to protect themselves against a future risk as long as the spending was reasonable and the potential risk was substantial.[187] The court already ruled that the potential risk was substantial in its injury in fact analysis. Therefore, the money plaintiffs spent to protect against identity theft was able to satisfy the redressability element. Since all three elements of standing were met by the plaintiffs, the court ruled that the plaintiffs "cleared the low bar to establish their standing at the pleading stage."[188]

IV. DISCUSSION

Together, the *Beck* and *AFGE* cases demonstrate how and why the federal circuit courts may fall on opposite sides of the split. The split remains highly contested in part due to a fear that granting standing to plaintiffs based on a future risk of identity theft will open the floodgates to massive class action litigation every time a data breach occurs.[189] However, taken together, the *Beck* and *AFGE* cases also illuminate the similarity of the factors that federal circuit courts use to decide whether to grant standing based of the risk of future identity theft. This Section shows that the factors the courts are weighing in these cases are the same regardless of how the courts ultimately rule. By using the factors that the federal circuit courts have already been using to justify their holdings, courts may be able to set a more cognizable threshold standard for standing in these types of cases. By doing so, courts will not need to turn away all plaintiffs who have been potentially injured while also avoiding a complete opening of the floodgates to litigation anytime there is a data breach. Instead, it is the facts and circumstances of each case, weighed with the factors the courts have already been using, that should determine whether or not a plaintiff is granted standing due to a risk of future identity theft. Next, this Section discusses the common factors used by the courts and explains how the factors are viewed similarly by the different courts. Last, this section proposes a line of questioning courts should adopt when deciding whether it is appropriate to grant standing based on a future risk

185. *Id.*

186. *Id.*

187. *Id.* at 61.

188. *Id.*

189. Omer Tene, *Neiman Marcus May Open the Floodgates for Breach Lawsuits*, INT'L ASS'N OF PRIVACY PROFS. (IAPP) (Jul. 24, 2015), https://iapp.org/news/a/neiman-marcus-may-open-the-floodgates-for-breach-lawsuits/ [https://perma.cc/Y9EB-YQXB].

of identity theft.

A. Intent of the Theft

In analyzing standing, the *Beck* and *AFGE* courts prioritized discussing the intent of the theft. Also, both cases approvingly cited to *Remijas*' language that "the purpose of the hack is, sooner or later, to make fraudulent charges."[190] Ultimately, this language suggests that "bad intent" may be implied in a traditional computer system hacking case. However, the language of *Remijas* is specific to a hack, and not all risk of future identity theft claims result from a stereotypical hack. There are also cases such as *Beck* that involve the theft of something tangible that may also threaten individuals' PII. For example, similar facts could arise from a stolen cell phone. In *Beck*, the court looked at the Sixth,[191] Seventh,[192] and Ninth[193] Circuit decisions that granted standing and specifically distinguished those case by noting the *Beck* theft did not possess the same intent that could be inferred from the stereotypical information systems hacks that were prevalent in the aforementioned cases.[194] In cases where intent cannot be implied simply by the act of the hack itself, something else is needed to confer the malicious intent of the hacker.

Both *AFGE* and *Beck* naturally looked next to whether any of the alleged victims' PII had been wrongfully used. This is a logical next question to ask because, if PII was wrongfully used, then it again makes sense to infer that the thief stole the information to use it for wrongful purposes. In cases like *Beck*, it may be unclear whether the thief stole the laptop to sell the laptop itself and make money, or if the thief stole the laptop for the purpose of using the PII the thief knew was stored on the laptop. Clearly, the latter scenario is much more likely to lead to future identity theft than the former. Generally, both sides of the split seem to agree that intent may be inferred through the breach itself in most situations where a traditional information systems breach occurs. If, however, the facts and circumstances of the specific incident do not make this inference clear, courts should next look to whether any victims' PII has already been wrongfully used. If misuse has occurred, courts may infer that, at a minimum, one of the hacker's goals was to misuse the information, which again allows courts to infer a substantial risk.

190. Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017); *AFGE*, 928 F.3d at 56.
191. Galaria v. Nationwide Mut. Ins. Co., 663 Fed. Appx. 384, 386 (6th Cir. 2016).
192. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015).
193. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632 (7th Cir. 2007).
194. *Beck*, 848 F.3d at 274.

B. Type of Information Stolen

Both *Beck* and *AFGE* also looked at the type of information that was at risk of being used incorrectly to determine whether the future risk of identity theft was substantial. Often, a significant amount of PII obtained through the theft may already have been freely available through other methods, such as the public domain. For example, names and addresses are often already in the public domain through public records. Even information such as someone's occupation or date of birth may be available from credit reports or social media websites such as Facebook or LinkedIn. The *Spokeo* Court specifically suggested (in the case of a statutory violation) that information such as a person's zip code may not satisfy the concreteness demands of Article III because an inaccurate zip code alone was not a risk of real harm.[195]

In the Eighth Circuit's *In re SuperValu, Inc., Customer Data Security Breach Litigation*[196] decision, the court held that credit card information, with no other PII stolen, is not enough to confer standing under Article III.[197] In that case, the court focused particularly on the types of PII data stolen to determine whether plaintiffs had standing.[198] Essentially, the type of information stolen determines whether the degree of risk is sufficient to meet the concreteness requirement of standing.

In *Beck* and *AFGE*, social security numbers were amongst the types of information stolen.[199] Social security numbers, unlike zip codes, are generally considered incredibly private and often unlock the ability to perform a plethora of financial activities such as opening, closing, and accessing bank accounts, credit cards, and loans. From a practical standpoint, a stolen social security number is a much larger burden on potential victims because social security numbers are much harder PII to change once they are compromised. The *AFGE* court viewed social security numbers, in addition to the surmountable other types of PII stolen, as sufficient to allow the simple inference that the type of information stolen in the breach was adequate to successfully commit identity theft.[200] The *Beck* court did not specifically comment on whether it believed the information on the laptop was sensitive enough to imply a risk is of future harm. However, the *Beck* court also did not attack the reasoning of the Sixth, Seventh, and Ninth Circuit courts which did infer

195. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549-50 (2016).

196. 870 F.3d 763 (8th Cir. 2017).

197. *Id.* at 771-72. (stating that credit card information was insufficient to support standing. Importantly, in that case, no other PII was allegedly stolen.).

198. *Id.* at 769-71.

199. *Beck*, 848 F.3d at 268; *AFGE* v. OPM (*In re* United States OPM Data Sec. Breach Litig.), 928 F.3d 42, 50 (D.C. Cir. 2019).

200. *AFGE*, 928 F.3d at 60.

that the information stolen was sufficiently sensitive. Instead, *Beck* focused on the intent of the hacker to distinguish the cases.[201] Therefore, between the two cases, it appears that social security numbers, along with some other types of stolen PII, are concrete enough to qualify as injury in fact. However, the *Beck* court's reasoning seemed to prioritize the thief's intent over the type of PII stolen by the thief.[202]

C. Timing

Perhaps the most controversial factor that the courts considered in *Beck* and *AFGE* was the role that the passage of time plays as a factor for determining whether a future risk is substantial. In their respective opinions, both circuit courts agreed that "as a general principle … as breaches fade further into the past … threatened injuries become more and more speculative."[203] The courts' statements on timing suggest that both courts understood timing to minimally be a factor worthy of consideration by courts, before either granting or denying standing. Although there may be an inferred agreement that courts believe timing should be a factor, both courts' opinions offer minimal guidance for understanding how significant of a factor the respective courts believe timing should be when deciding whether a plaintiff has standing.

The *Beck* opinion noted it had been over three years since the initial data breaches and still no evidence existed of actual identity theft.[204] Since the thief in *Beck* was not a traditional information systems hack, but instead involved the theft of a laptop, the court could not infer the thief's intent by the act of the theft itself, like it suggested one could with cases involving a traditional data hack.[205] The court then used the passage of time as a detrimental fact against the plaintiffs. The court believed the prolonged timespan between the theft and the case, without an incident of identity theft, made the inference that the thief's intent was to use the PII for identity theft a much more speculative inference. Essentially, the *Beck* court used the passage of time as a weighing factor when intent of the thief could not be inferred by the act of the theft itself.

Lastly, it should be noted that the *Beck* court only discussed passage of time under its "certainly impending" analysis.[206] In many ways, it makes sense that the passage of time may play a larger role determining whether a plaintiff has standing in cases that involve the stricter "certainly

201. *See Beck*, 848 F.3d at 274-75.

202. *Id.*

203. *AFGE*, 928 F.3d at 59. (quoting *Beck,* 848 F.3d at 275).

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

205. *See* discussion *supra* Section IV.A.

206. *Beck*, 848 F.3d at 274-75.

impending" standard, compared to the more laxed "substantial risk" standard. Under the *Clapper* analysis, it is evident that at least part of what makes "certainly impending" a higher bar for plaintiffs to pass is that there in an immediacy to something being "certainly impending" as opposed to there merely being a "substantial risk" of something happening in the future.

The *AFGE* court analyzed the passage of time factor under facts that the court believed allowed it to infer intent of the theft by the act of the hack itself. Therefore, the *AFGE* court examined timing as an independent factor, instead of merely being a factor used to infer a thief's intent, like the *Beck* court did. Although the court still admitted passage of time played some role in determining a future risk of identity theft, overall the court was reluctant to give the factor much weight. First, the court mostly declined to analyze the issue by stating it believed it was too early to make a determination regarding timing because of the large scale of the data breach and the relative novelty of large-scale data breaches, generally.[207] Essentially, the court believed it did not possess enough knowledge about the general workings of data breaches and therefore did not want to make any substantive rulings on data breaches related to how the passage of time may or may not affect the substantiality of the risk of future identity theft. Second, the only significant position the court held on timing at all was that it was unpersuaded that two years between the cyberattacks and the lawsuit was a long enough passage of time to make the threat insubstantial.[208] All in all, *AFGE* did acknowledge that the passage of time may play a role in the standing analysis but limited the factor by (1) stating two years was not a long enough passage of time to affect the analysis, and (2) showing a general reluctance to giving the factor much weight.[209]

D. Certainly Impending v. Substantial Risk: Which Standard Applies?

The previously discussed factors of intent, timing, and type of PII stolen from the theft likely allow for much more elastic inferences when analyzed under the "substantial risk" standard versus the "certainly impending" standard. Since *Clapper*, courts have suggested the certainly impending test may only relate to matters of national security or facial challenges.[210] Courts' treatment of the two standards since *Clapper* unquestionably shows a willingness to use the substantial risk standard in

207. *AFGE*, 928 F.3d at 59.

208. *Id.*

209. *Id.*

210. Stevens v. Zappos.com, Inc. (*In re* Zappos.com, Inc., Customer Data Sec. Breach Litig.), 884 F.3d 893, 897-98 (9th Cir. 2018).

lieu of its alternative.[211] The Supreme Court could clarify when each standard is preferred by granting a writ of certiorari on a related case. Without a Supreme Court clarification, appellate courts have consistently shown a respect for the substantial risk standard by often using the standard for their standing analyses. It is almost impossible for individuals to know exactly when their PII may become compromised after a data breach. Further, it is also nearly impossible for a victim to know whether a thief intends to misuse their PII or what a thief's comprehension skills are for both understanding and wrongfully using an individual's data. Due to an alleged victim's inability to know these facts, it is logical, in most cases, to apply the more lenient standard when determining standing. Lastly, the *SBA List* decision following *Clapper* also further illustrates the Supreme Court's willingness to use the more lenient substantial risk standard. Together, these factors make the substantial risk standard the desired standard for courts to use when determining standing based on a future risk of identity theft.

E. Resulting Standard for Courts Moving Forward

Using the factors previously discussed, the circuit courts' rulings in *Beck* and *AFGE* offer guidance for other courts to analyze the circuit split without simply granting or denying standing in all cases involving a future risk of identity theft. In fact, the cases demonstrate that as circuit courts' jurisprudence on the split has continued to evolve, consistent factors have arisen in appellate decisions and may now be synthetized and used to analyze the split henceforward. The following is an order of questions courts should ask to determine if a plaintiff has standing based on a future risk of identity theft.

First, a court must figure out which standard to apply: "certainly impending" or "substantial risk." Based on *Clapper*, courts know that if there is a question of national security or a separation of powers question at issue, courts should apply the certainly impending standard. A question of separation of powers is more likely to arise in a case that facially challenges a statute. Naturally, a facial challenge positions a court against a decision by Congress. In an effort to show deference to the decisions of Congress, it makes sense to require that plaintiffs pass a stricter standing requirement in those cases. Based on a broader implementation of *Clapper*, the certainly impending standard could be required in any cases involving the federal government. However, *AFGE* involved a federal government agency and the court did not require plaintiffs to pass the

211. As previously discussed, *SBA List*, *Attias*, *AFGE*, *Remijas*, and *Zappos.com*, *Inc*. all use the "substantial risk" standard in their analyses.

stricter certainly impending standard. Therefore, moving forward, other courts should follow suit and freely apply the substantial risk standard in all cases that do not involve national security or separation of powers issues, like the Supreme Court did in *SBA List*.

After deciding which standard applies, the type of information stolen serves as a gateway to the rest of the standing analysis. Both *Beck* and *AFGE* dealt with the theft of social security numbers along with other types of identifying PII. Taking a holistic view, courts need to simply ask if the type of PII stolen, judged altogether, allow for a relatively competent thief to commit identity theft. After *Beck* and *AFGE*, courts should consider social security numbers with minimal other PII sufficient for a relatively competent theft to commit identity theft. Whether credit card numbers or bank account numbers along with other pieces of PII pass the same test is likely dependent on the facts and circumstances of the theft and the intent of the thief.

Next, courts should turn to analyzing the intent of the thief. Based on *Beck*'s and *AFGE*'s favorable treatment of the logic used in *Remijas*, if the theft occurred via a traditional data hack, ill-will on behalf of the hacker may be implied. If the theft occurred by means other than a data hack, then courts should next determine whether some of the alleged victims' information was actually misused after the theft. In *AFGE*, later actual misuse was a supporting factor for the plaintiffs. In *Beck*, no evidence of a later misuse was a negating factor for the plaintiffs. Overall, if PII was stolen, and later misused, then standing should be granted.

On the other hand, if there has not been any later misuse, courts should then turn to the passage of time factor. The *AFGE* court examined the passage of time as a possible independent factor. But by stating that the court did not believe it was in a position to substantially rule on timing, due to the relatively contemporaneous nature of large-scale data breaches, the effect was to essentially neuter the factor of any persuasive weight. However, the *Beck* analysis may offer a more natural fit for where to structure timing as a factor in the overall standing analysis; timing is best examined when the thief's intent cannot be easily inferred by the act. If a significant time has passed since the act, no misuse of the information has been reported by any of the plaintiffs, and the intent of the thief may not be inferred based on the type of theft, then courts should follow the decision of the *Beck* court and not grant standing to the plaintiff.

Notwithstanding the above guidance, questions still persist regarding how to best determine when the passage of time becomes significant. Neither the *Beck* nor *AFGE* decision provides much guidance for how to determine when the amount of time elapsed since a theft becomes significant. Based on *AFGE*, two years may not be enough time to be considered significant, at least when dealing with a large-scale data

breach that potentially affects millions of people's PII. The laptop in *Beck* was stolen about three and a half years prior to when the Fourth Circuit heard the case and affected approximately 7,400 patients.[212] Together, it may be deduced that the passage of time factor may be elastic, depending on the amount of PII stolen and people affected. As guideposts, two years may not be long enough, but more than three years could be considered a significant amount of time.

V. CONCLUSION

As the number of data breaches in the United States continue to rise, surely so will the amount of litigation concerning how to best make victims of subsequent identity theft whole. As individuals continue to adapt to the rapidly progressing digital age, individuals will become even more keenly aware of the potential financial risks that threaten them after their PII is stolen. People who find out their PII has been compromised will likely continue to file claims against the entities who failed to protect their PII.

Those realities put federal courts in a tough spot: do federal courts flood the courts by encouraging individuals to take proactive measures to protect themselves from potentially significant financial losses and grant standing based off of a future risk of identity theft? Or do courts protect the judicial systems from a flood of litigation dealing with the growing issue by not granting standing to plaintiffs until actual identity theft occurs? The Supreme Court has not directly resolved this issue.

Thankfully though, recent decisions falling on either side of the circuit split have provided guidance as to what factors matter most when federal courts resolve cases based on a future risk of identity theft. The type of information stolen and the thief's intent have surfaced as the two most important factors. Furthermore, within intent, courts may look to whether identity theft has already occurred amongst the plaintiffs and the passage of time to determine if the risk is "certainly impending" or a "substantial risk." By potentially leaving the door to litigation open, one may argue that the courts will still be swamped with litigation. However, by adopting the framework of questions discussed in Section IV, courts should be able to clarify the factors and effectively limit the amount of overall litigation on the subject, while still allowing plaintiffs who proactively incurred costs to mitigate future damages the ability to be made whole for costs they responsibly incurred.

212. *Beck*, 848 F.3d at 267.