Risky Business: The Risk of Identity Theft and Standing to Sue

Parker Hudson*

ABSTRACT

Nearly one in five Americans will experience an incident of identity theft during their lifetimes, often as the result of a data breach. These victims come from all different backgrounds, their assailants are indiscriminate. In a time where technology is making it easier than ever for identity thieves to harm people from afar, the law must similarly evolve to protect these victims from further injury.

The Supreme Court has recognized that the threat of future injury may be sufficient to confer standing to sue in an Article III federal court. However, the Court's precedent is strained where the alleged injury is the increased risk of future identity theft following a data breach. Unsurprisingly, the circuit courts are split on whether the risk of future identity theft is sufficient to confer Article III standing.

Congress has yet to enact legislation providing data-breach victims with a private cause of action against the party responsible for their data's vulnerability. However, other countries, unions, and several states have enacted such legislation. Notably, the European Union and California have both addressed the issue with robust statutes.

This Comment highlights the magnitude of risk that consumers face when data breaches compromise their personal identifiable information. It also discusses the General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"), statutes enacted by the European Union and California, respectively. Ultimately, this Comment argues: (1) that the Supreme Court should take a consumer-minded approach in resolving the current circuit split, and (2) that Congress should enact legislation providing data-breach victims with standing to sue the parties responsible for their data's exposure, while striking a compromise between the GDPR and the CCPA.

* J.D. Candidate, The Pennsylvania State University, Penn State Law, 2021.

Table of Contents

I. INTRODUCTION 534
II. BACKGROUND 536
A. Defining "Personal Identifiable Information" 537
B. Establishing Standing Under Article III 537
C. Future Injury and Standing in Supreme Court Precedent 539
1. *Clapper v. Amnesty International USA* 540
2. *Spokeo, Inc. v. Robins* 542
D. The Circuit Split: Finding Article III Standing Where the Claimed Injury-in-Fact is the Substantial Risk of Future Identity Theft 544
1. The D.C. Circuit 544
a. *American Federation of Government Employees v. U.S. Office of Personnel Management* 544
b. *Attias v. CareFirst, Inc.* 546
2. The Seventh Circuit 547
3. The Sixth Circuit 548
4. The Fourth Circuit 550
5. The Eighth Circuit 551
6. Summary of the Circuit Split 553
E. Examining Existing Data-Privacy Law 554
1. The General Data Protection Regulation 554
2. The California Consumer Privacy Act of 2018 556
III. ANALYSIS 557
A. The Supreme Court 558
B. Congress Must Enact Comprehensive Data-Privacy Legislation 559
C. Recommendation 562
IV. CONCLUSION 563

I. INTRODUCTION

According to the Identity Theft Resource Center ("ITRC"),[1] data breaches compromised 446,515,334 consumer personal-identifiable-information ("PII") records in 2018.[2] This number represents a 126% increase from the number of records compromised in 2017.[3] Together exposing 420,928,055 records, hacking and unauthorized access were the

1. The ITRC is a non-profit organization established to support victims of identity theft. *See generally* 2018 END-OF-YEAR DATA BREACH REPORT, IDENTITY THEFT RESOURCE CTR. (2019), https://bit.ly/36FFPRQ [hereinafter *2018 REPORT*].

2. *See id.*

3. *See id.*

most common forms of data breaches.[4] The "Business" sector experienced the most considerable number of data breaches, followed by the "Government and Military" sector.[5] According to the ITRC's report, only one-half of the breach victims disclosed the number of compromised records.[6] Notably, when an entity reports a breach to the ITRC but fails to report the number of compromised records, the ITRC does not speculate about the number of records exposed.[7] Accordingly, the actual number of records compromised by data breaches is presumably higher than the number reported.[8]

Once PII has been compromised, the perpetrator in possession of the PII may leverage the information in nefarious ways, such as stealing the victim's identity and using the stolen identity to commit crimes or executing fraudulent transactions with the victim's financial information.[9] Victims of PII-compromising breaches are often able to sue the responsible party.[10] However, where the claimed injury is the substantial risk of *future* identity theft, victim plaintiffs experience drastically different results depending on the forum in which they sue.[11] For example, a breach victim's claim may survive a motion to dismiss in one jurisdiction, but fail to overcome a motion to dismiss in another jurisdiction, which effectively nullifies their claim.[12]

---

4. *See id.* Hacking accounted for 39% of breaches, unauthorized access accounted for 30% of breaches. *See id.*

5. The Business sector lost 415,233,143 records in 571 breaches, the Government and Military sector lost 18,236,710 records in 99 breaches. *See id.*

6. *See id.* ("Only half of the total number of breaches reported by the [ITRC] in 2018 reported the number of records exposed.").

7. *See id.* ("[T]he ITRC . . . [does] not include an educated guess or 'possible' number of records to ensure that [they are] providing the best data quality.").

8. *See id.* ("The actual number of exposed records likely exceeds the reported number substantially.").

9. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is . . . to make fraudulent charges or assume those consumers' identities.").

10. *See* Michael Hopkins, Comment, *Your Personal Information Was Stolen? That's an Injury: Article III Standing in the Context of Data Breaches*, 50 U. PAC. L. REV. 427, 430 (2019) ("These data breaches frequently lead to lawsuits.").

11. *Compare* Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42, 61 (D.C. Cir. 2019) (holding that "plaintiffs have plausibly alleged a substantial risk of future identity theft that is fairly traceable to OPM's . . . failings and [is] likely redressable"), *with* Reilly v. Ceridan Corp., 664 F.3d 38, 46 (3d Cir. 2011) (holding that "[Plaintiffs] failed to . . . demonstrate standing to bring this suit under Article III, because [Plaintiffs'] allegations of an increased risk of future identity theft as a result of the security breach are hypothetical, future injuries, and are therefore insufficient to establish standing").

12. *Compare Am. Fed'n of Gov't Emps.*, 928 F.3d at 75 (holding that Plaintiffs adequately alleged Article III standing and reversing the trial court's granting of Defendant's motion to dismiss for lack of standing), *with Reilly*, 664 F.3d at 46 (holding

Part II begins with a discussion of PII and Article III's standing requirement, which determines whether a claimant can bring suit in federal court.[13] Part II then examines existing Supreme Court precedent on future harm and Article III standing.[14] Then, Part II discusses the existing circuit split regarding whether the risk of future identity theft is a sufficient injury-in-fact for Article III standing purposes.[15] Part II concludes by discussing existing data-privacy laws, including the General Data Protection Regulation[16] and the California Consumer Privacy Act,[17] enacted by the European Union and California, respectively.[18]

Part III analyzes the existing circuit split against the backdrop of Supreme Court precedent and recommends that the Supreme Court determine whether the risk of future identity theft is a sufficient injury-in-fact for Article III purposes.[19] Part III then analyzes the GDPR and the CCPA before, ultimately, recommending that Congress enact legislation that strikes a compromise between consumer and business interests.[20] Lastly, Part IV emphasizes the importance and need for clarity from the Supreme Court and Congress on the issue of whether data-breach victims have standing to sue where the alleged injury is the risk of future identity theft.[21]

II. BACKGROUND

Businesses use their consumers' personal identifiable information ("PII") for many reasons, such as adjusting marketing strategies, improving the consumer experience, and creating revenue.[22] Unfortunately, businesses often fail to shield their consumers' PII from data breaches.[23] Once in the hands of the wrong person, PII can be put to a host of evil uses, including identity theft.[24] The following Section

---

that Plaintiffs failed to allege Article III standing and affirming the trial court's granting of Defendant's motion to dismiss for lack of standing).

13. *See infra* Sections II.A–B.

14. *See infra* Sections II.C.1–2.

15. *See infra* Sections II.D.1–6.

16. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119) (EU).

17. CAL. CIV. CODE Div. 3, Pt. 4, Title 1.81.5 (Deering 2018).

18. *See infra* Sections II.E.1–2.

19. *See infra* Section III.A.

20. *See infra* Sections III.B–C.

21. *See infra* Part IV.

22. *See* Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (Aug. 3, 2018), http://bit.ly/2SRJF1F.

23. *See 2018 REPORT*, *supra* note 1.

24. *See Safeguarding Your PII*, IDENTITY THEFT RESOURCE CTR. (July 20, 2017), http://bit.ly/2V2I4Jr.

defines PII before turning to the specific constitutional requirements that data-breach victims must meet to sue in federal court.

A. Defining "Personal Identifiable Information"

The United States Department of Labor defines PII as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[25] Information that could be used to identify an individual directly includes the individual's name or social security number.[26] Information that could be used to identify an individual indirectly includes the individual's gender or race.[27]

Once a data breach compromises PII, breach victims facing the risk of future identity theft must establish that they have standing to sue the responsible party.[28]

B. Establishing Standing Under Article III

Article III of the U.S. Constitution[29] confines the jurisdiction of federal courts to a limited number of "cases" and "controversies."[30] To satisfy Article III's case-or-controversy requirement—triggering a federal court's authority to adjudicate a complaint—a complainant must establish his or her "standing."[31]

Standing refers to the constitutional requirements a complainant must meet to be eligible to sue in federal court.[32] Rooted in separation-of-powers principles, the requirements prevent complainants from using

25. *Guidance on the Protection of Personal Identifiable Information*, U.S. DEP'T LAB., http://bit.ly/31avarS (last visited Oct. 11, 2020).

26. *See id.* (providing "name, address, social security number or other identifying number or code, telephone number, email address, etc." as means of directly identifying an individual).

27. *See id.* (providing "gender, race, birth date, geographic indicator, and other descriptors" as means of indirectly identifying an individual).

28. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013) (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997)) ("One element of the 'case-or-controversy' requirement is that plaintiffs 'must establish that they have standing to sue.'").

29. U.S. CONST. art. III.

30. U.S. CONST. art. III, § 2, cl. 1.; *see also Clapper*, 568 U.S. at 408 (quoting Daimler Chrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006)) ("[N]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.").

31. *See Clapper*, 568 U.S. at 408 (quoting *Raines*, 521 U.S. at 818) ("One element of the 'case-or-controversy' requirement is that plaintiffs 'must establish that they have standing to sue.'").

32. *See* Thomas Martecchini, Note, *A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft After* Clapper v. Amnesty International USA, 114 MICH. L. REV. 1471, 1475 (2016) ("The standing doctrine defines who can bring suit for a particular claim.").

the judicial system to bypass other branches of government.[33] Additionally, standing ensures that the complainant has a "personal stake in the outcome of the controversy."[34] "The irreducible constitutional minimum of standing consists of three elements": (1) injury-in-fact, (2) causation, and (3) redressability.[35]

First, a complainant must demonstrate that they suffered an injury-in-fact.[36] Federal courts use a two-prong test to evaluate whether an alleged injury constitutes injury-in-fact.[37] The alleged injury must be: (1) "concrete and particularized," and (2) "actual or imminent, not conjectural or hypothetical."[38] The Supreme Court has clarified that "concrete" is intended to mean real harm,[39] and a "particularized" injury is one that affects the individual in a personalized way.[40] An allegation of future injury can satisfy the imminence requirement if the claimed injury is "certainly impending" or if there is a "substantial risk" that the harm will occur.[41]

Second, the complainant must demonstrate causation.[42] To satisfy the causation requirement, Article III requires that the claimed injury be "fairly traceable" to the defendant.[43] The defendant does not need to be "the most immediate cause, or even a proximate cause" of the claimed injury, as long as the injury can be attributed to the defendant somehow.[44]

Lastly, the complainant must establish that the injury is redressable by a favorable decision.[45] Courts will not find standing if they cannot remedy the complainant's injury by ruling in the complainant's favor.[46]

For victims of a data breach who have lost PII and are alleging a substantial risk of future identity theft, Article III's injury-in-fact requirement often proves to be the most challenging hurdle to clear.[47]

---

33. *See Clapper*, 568 U.S. at 408.

34. Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014).

35. *See* Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42, 54 (D.C. Cir. 2019) (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

36. *See id.* at 54.

37. *See id.*

38. *See id.* (quoting *Spokeo*, 136 S. Ct. at 1548).

39. *See Spokeo*, 136 S. Ct. at 1549.

40. *See id.*

41. *See* Susan B. Anthony List v. Driehaus, 573 U.S. 149, 158 (2014) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 (2013)).

42. *Am. Fed'n of Gov't Emps.*, 928 F.3d at 54.

43. *See id.* (quoting Attias v. Carefirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017)).

44. *See id.*

45. *See id.*

46. *See id.*

47. *See* Douglas H. Meal, *Private Data Security Breach Litigation in the United States*, ASPATORE, Jan. 2014, at 1, 2 ("[A] plaintiff must show that he or she suffered some appreciable, non-speculative, present harm to state a claim for relief. So far, no element has proven more elusive for plaintiffs."); Brandon Ferrick, Comment, *Annual*

The Supreme Court has not directly addressed what facts a data-breach victim must allege during the pleading stage of litigation in order to survive a motion to dismiss. Still, the Supreme Court's decisions in *Clapper v. Amnesty International USA*[48] and *Spokeo, Inc. v. Robins*[49] have been applied by federal district and circuit courts when determining whether a complainant's claimed risk of future identity theft is sufficient for standing purposes.[50]

Clapper is considered the leading case on whether a claimed future injury is sufficiently "imminent" to satisfy the injury-in-fact requirement.[51] Similarly, *Spokeo* is considered the leading case on whether a claimed future injury is sufficiently "concrete and particularized"[52] to satisfy the injury-in-fact requirement.[53]

C. Future Injury and Standing in Supreme Court Precedent

The Supreme Court considered whether the risk of a future injury is sufficient to satisfy Article III's injury-in-fact requirement in *Clapper* and *Spokeo*.[54]

Clapper involved a group of plaintiffs seeking to strike down a federal statute as unconstitutional.[55] After determining that the complainants' risk of future injury was highly speculative and not sufficiently imminent, the Court in *Clapper* held that the complainants failed to establish standing.[56]

Spokeo arose out of a purported violation of the Fair Credit Reporting Act.[57] There, the Court clarified that an alleged injury must be

---

Survey of Federal En Banc and Other Significant Cases: No Harm, No Foul: The Fourth Circuit Struggles with the "Injury-in-Fact" Requirement to Article III Standing in Data Breach Class Actions, 59 B.C.L. REV. E-SUPP. 462, 469 (2018) ("In data breach cases, the injury-in-fact element is often the most contentious.").

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

49. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

50. *See* Attias v. CareFirst, Inc., 865 F.3d 620, 626 (D.C. Cir. 2017) ("As the district court recognized, the leading case on claims of standing based on risk of future identity is *Clapper* . . . .").

51. *See Recent Case: Cyberlaw – Data Breach Litigation – D.C. Circuit Holds That Heightened Risk of Future Injury Can Constitute an Injury in Fact for Article III Standing.* – In re. U.S. Office of Personnel Management Data Security Breach Litigation, *928 F.3d 42 (D.C. Cir 2019)*, 133 HARV. L. REV. 1095, 1099 (2020) [hereinafter *Cyberlaw*].

52. Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42, 54 (D.C. Cir. 2019) (quoting *Spokeo*, 136 S. Ct. at 1547).

53. *See Cyberlaw*, *supra* note 51, at 1099.

54. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); *see also Spokeo*, 136 S. Ct. at 1540.

55. *See Clapper*, 568 U.S. at 401.

56. *See id.* at 410.

57. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018); *Spokeo*, 136 S. Ct. at 1546.

both "concrete" and "particularized," articulating that the two represent distinct requirements, rather than an individual requirement.[58]

1. *Clapper v. Amnesty International USA*

Congress passed the Foreign Intelligence Surveillance Act (FISA)[59] in the wake of the Supreme Court's decision in *United States v. United States District Court for Eastern District of Michigan*, also known as the "*Keith*" case.[60] In *Keith*, the Court recognized that the "standards and procedures that law enforcement officials must follow when conducting 'surveillance of "ordinary crime"' might not be required in the context of surveillance conducted for domestic national-security purposes."[61] Aimed at improving foreign intelligence, the FISA authorized the government to conduct surveillance of certain foreign communications.[62]

Congress created several procedural safeguards to ensure that the FISA was constitutionally permissible.[63] Notably, Congress established the Foreign Intelligence Surveillance Court ("FISC").[64] The FISC could authorize surveillance for intelligence purposes only after finding probable cause that the surveillance target was a "foreign power or an agent of a foreign power."[65]

Shortly after the September 11, 2001 terrorist attacks, President George W. Bush[66] encouraged Congress to amend the FISA to "provide the intelligence community with additional authority to meet the challenges of modern technology and international terrorism."[67] In accord with President Bush's request, Congress passed the FISA Amendments Act of 2008 ("FISA Amendments Act").[68] Section 1881a of the FISA Amendments Act abrogated the above-mentioned probable cause requirement.[69] Further, Section 1881a displaced the requirement that the government specify the "nature and location of each of the

58. *See Spokeo*, 136 S. Ct. at 1548–49.

59. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783.

60. *See Clapper*, 568 U.S. at 402 (citing United States v. United States Dist. Court for Eastern Dist. of Mich., 407 U.S. 297, 322–23 (1972)).

61. *Id.* (quoting *United States Dist. Court for Eastern Dist. of Mich.*, 407 U.S. at 322–23).

62. *See id.* at 402–403.

63. *See id.*

64. *Id.* at 403.

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

66. George W. Bush was the President of the United States from 2001–2009. *George W. Bush*, WHITE HOUSE, https://bit.ly/3lsxpkT (last visited Oct. 11, 2020).

67. *Clapper*, 568 U.S. at 403.

68. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436 (2008); *Clapper*, 568 U.S. at 403.

69. *See Clapper*, 568 U.S. at 403.

particular facilities or places at which the electronic surveillance will occur."[70]

Shortly after Congress passed the FISA Amendments Act, a group of individuals sought to contest the FISA Amendments Act as unconstitutional.[71] The work that these individuals performed required their communication with people the individuals believed were targets of surveillance authorized by the FISA Amendments Act.[72] These individuals sought to satisfy Article III's injury-in-fact requirement by asserting that they faced an "objectively reasonable likelihood that their communications" would be intercepted pursuant to Section 1881a of the FISA Amendments Act.[73]

Writing for the majority, Justice Alito stated that the Court's standing inquiry is "especially rigorous when reaching the merits of the dispute would force [it] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."[74] Justice Alito added that the Court seldom finds standing in cases where it is asked to review actions concerning foreign intelligence.[75]

Explaining that the complainants' reliance on an "objectively reasonable likelihood" standard was fatal to their claimed injury-in-fact, the majority held that the complainants failed to establish Article III standing.[76] The Court reasoned that the complainants relied on a highly attenuated, speculative chain of events to prove their claimed future injury.[77] Justice Alito reiterated that the "threatened injury must be certainly impending to constitute injury-in-fact and . . . allegations of possible future injury are not sufficient" to meet Article III's injury-in-fact requirement.[78] Significantly, the Court later clarified that:

> [Supreme Court jurisprudence] does not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, [the Court has] found standing

70. *Id.*
71. *See id.* at 401.
72. *See id.*
73. *See id.*
74. *Id.* at 408 (quoting Raines v. Byrd, 521 U.S. 811, 818 (1997)).
75. *See id.* at 409.
76. *See id.* at 410.
77. *See id.* ("[R]espondents' argument rests on their highly speculative fear that: (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under § 1881a rather than utilizing another method of surveillance; (3) Article III judges who serve on the FISC will conclude that the Government's proposed surveillance procedures satisfy § 1881a's many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.").
78. *Id.* at 409 (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

> based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.[79]

However, Justice Alito added that, even if the substantial risk standard were applicable, the complainants' alleged injury fell short of this standard, considering the attenuated, speculative chain of events necessary to establish harm.[80]

Having explained in *Clapper* the imminence prong of the two-prong injury-in-fact analysis,[81] the Court, in *Spokeo*, turned to the "concrete and particularized" prong.[82]

2. *Spokeo, Inc. v. Robins*

Spokeo, Inc. ("Spokeo") operated a people search engine.[83] Users could query Spokeo's database for information about an individual.[84] Available information included age, marital status, level of education, employment status, and relative financial standing.[85] A Spokeo user generated a report about Robins, the complainant.[86] According to Robins, the report contained inaccurate information.[87] Robins filed suit against Spokeo alleging violations of the Fair Credit Reporting Act ("FCRA"), which requires that "consumer reporting agenc[ies]," such as Spokeo, take reasonable measures to assure consumer reports contain the highest level of accuracy.[88]

At the trial court level, Spokeo prevailed in having Robins' complaint dismissed for failure to allege an injury-in-fact.[89] However, on appeal, the Ninth Circuit reversed, stating that Spokeo's violation of the FCRA was a sufficient injury-in-fact to confer standing.[90] The Supreme Court granted certiorari to address whether the Ninth Circuit had erred in its injury-in-fact analysis, ultimately remanding after deciding that the Ninth Circuit's analysis was incomplete.[91]

---

79. *Clapper*, 568 U.S. at 414 n.5 (referencing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153 (2010)).
80. *See id.*
81. *See id.* at 409–10, 414 n.5.
82. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–49 (2016).
83. *See id.* at 1544.
84. *See id.*
85. *See id.* at 1546.
86. *See id.* at 1544.
87. *See id.*
88. *See id.* at 1546.
89. *See id.*
90. *See id.*
91. *See id.* at 1546, 1550.

Justice Alito emphasized that an alleged injury must be both "concrete" and "particularized."[92] Alone, neither are sufficient because the two represent distinct requirements.[93] Relying on a plain-language interpretation, Justice Alito explained that, to be "concrete," the injury must actually exist.[94] However, Justice Alito clarified that a concrete injury does not necessarily need to be tangible.[95] Indeed, intangible injuries, such as the risk of real harm, may also be concrete.[96] Concerning particularity, Justice Alito explained that, for an injury to be "particularized," it must "affect the plaintiff in a personal and individual way."[97]

Because the majority determined that the Ninth Circuit failed to evaluate both concreteness and particularity, the Court did not address the imminence prong of the injury-in-fact analysis.[98] The Court remanded the case to the Ninth Circuit without addressing whether Robins' alleged injury was sufficient to confer standing.[99]

Unsurprisingly, federal district and circuit courts tasked with deciding whether the risk of future identity theft is sufficient to satisfy Article III's injury-in-fact requirement have struggled to apply the Court's decisions in *Clapper* and *Spokeo* with consistency.[100] *Clapper* concerned a federal statute that enabled the Government to conduct surveillance of certain foreign communications.[101] *Spokeo* concerned a purported violation of the FCRA.[102] Applying *Clapper* and *Spokeo* to instances of PII-compromising data breaches and the subsequent risk of identity theft is far from a perfect fit due to the highly specialized nature of each case. As such, courts tasked with determining whether an injury-in-fact exists for Article III standing in the PII context have reached mixed results.[103]

92. *Spokeo*, 136 S. Ct. at 1548 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

93. *See id.* at 1548.

94. *See id.*

95. *See id.* at 1549.

96. *See id.*

97. *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560 n.1).

98. *See id.* at 1550.

99. *See id.*

100. *See* Martecchini, *supra* note 32, at 1483 ("Following the Court's own uncertainty in Clapper as to the appropriate imminence standard, a number of district courts have reached contrasting conclusions regarding the viability of standing based on increased risk in data-breach cases.").

101. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

102. *See Spokeo*, 136 S. Ct. at 1546.

103. *See* Martecchini, *supra* note 32, at 1483.

D. The Circuit Split: Finding Article III Standing Where the Claimed Injury-in-Fact is the Substantial Risk of Future Identity Theft

Four circuit courts have found standing based on an increased risk of future identity theft.[104] Conversely, four circuit courts have refused to find standing based on an increased risk of future identity theft.[105] This Comment focuses its discussion on the circuits that addressed the issue after the Supreme Court's *Clapper* decision.[106] Generally, courts that have found standing in this context have taken a pro-consumer approach and underscored the nature of the data lost and the ultimate harm—identity theft—that victims face.[107] In contrast, courts that have not found standing have generally taken a business-friendly approach, relying on *Clapper* and finding the alleged harm too speculative.[108]

1. The D.C. Circuit

The D.C. Circuit considered whether the risk of future identity theft is sufficient to satisfy Article III's injury-in-fact requirement in *American Federation of Government Employees v. U.S. Office of Personnel Management*[109] and in *Attias v. CareFirst, Inc.*[110] In both cases, the D.C. Circuit held that the risk of future identity theft is sufficient to satisfy Article III's injury-in-fact requirement.[111]

a. *American Federation of Government Employees v. U.S. Office of Personnel Management*

In 2014, the U.S. Office of Personnel Management (OPM) was hacked.[112] Cyber assailants targeted databases that housed personal identifiable information ("PII"), including: social security numbers, birth dates, addresses, and fingerprint records.[113] In total, 21 million people

104. *See* Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42 (D.C. Cir. 2019); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 663 Fed. App'x. 384 (6th Cir., filed Sept. 12, 2016); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015); Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).

105. *See* Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017); Alleruzzo v. SuperValu, Inc., 870 F.3d 763, 766 (8th Cir. 2017); Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

106. *See infra* Sections II.D.1–5.

107. *See infra* Section II.D.6.

108. *See infra* Section II.D.6.

109. *See Am. Fed'n of Gov't Emps.*, 928 F.3d at 42.

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

111. *See id.* at 626; *see also Am. Fed'n of Gov't Emps.*, 928 F.3d at 53.

112. *See Am. Fed'n of Gov't Emps.*, 928 F.3d at 49.

113. *See id.*

were affected by the data breach.[114] Shortly after the data breach, victims of the breach whose PII was compromised brought suit against OPM.[115]

The lawsuits were consolidated into two complaints.[116] The National Treasury Employees Union ("NTEU Plaintiffs") filed one suit.[117] The American Federation of Government Employees ("Arnold Plaintiffs") filed a second.[118] According to the D.C. Circuit, both complainants alleged that "OPM's cybersecurity practices were woefully inadequate," which enabled cyber attackers to access the agency's "treasure trove" of employee PII, exposing the plaintiffs to a heightened risk of identity theft.[119] The district court rejected the complainants' arguments and dismissed both complaints for lack of standing.[120]

On appeal, the D.C. Circuit reviewed each consolidated complaint separately.[121] The court determined that the NTEU Plaintiffs had established Article III standing; however, their arguments are beyond the scope of this Comment.[122]

Concerning the Arnold Plaintiffs, the D.C. Circuit focused its Article III standing analysis on "[the] one injury [the Arnold Plaintiff's] all share: the risk of future identity theft."[123] The court considered the nature of the PII lost during the breach and noted that "[the hackers] . . . have in their possession all the information needed to steal Arnold Plaintiffs' identities."[124] Additionally, the D.C. Circuit acknowledged that several Arnold Plaintiffs had already experienced various types of identity theft.[125] These incidents supported the Arnold Plaintiffs' claim that they faced a substantial risk of future identity theft.[126] OPM argued

114. *See id.*
115. *See id.*
116. *See id.*
117. *See id.*
118. *See id.*
119. *See id.*
120. *See id.*
121. *See id.* at 54–61.
122. *See Am. Fed'n of Gov't Emps.*, 928 F.3d at 54. The NTEU Plaintiffs' argument centered on a "constitutional right to informational privacy," rather than the increased risk of future identity theft. *See id.*
123. *Id.* at 56.
124. *Id.* ("Arnold Plaintiffs have alleged that the hackers stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information.").
125. *See id.* ("[S]everal Arnold Plaintiffs claim that they have already experienced various types of identity theft, including the unauthorized opening of new credit card and other financial accounts and the filing of fraudulent tax returns in their names.").
126. *See id.* ("It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft. . . . [W]e conclude that [these incidents] support the inference that the Arnold Plaintiffs face a substantial—as opposed to merely speculative or theoretical—risk of future identity theft.").

that espionage, rather than identity theft, motivated the breach.[127] Reasoning that identity theft and espionage can coexist, the D.C. Circuit rejected this argument.[128]

After considering the nature of the data stolen and the various forms of identity theft already experienced by several plaintiffs after the breach, the D.C. Circuit determined that the Arnold Plaintiffs had sufficiently alleged facts to support their claimed injury.[129]

The D.C. Circuit also considered whether the risk of future identity theft was sufficient to satisfy Article III's injury-in-fact requirement in *Attias*.[130]

b. *Attias v. CareFirst, Inc.*

In 2014, CareFirst, a health insurer, fell victim to a data breach.[131] In total, the cyber assailant breached 22 computers and accessed a database containing customers' PII.[132] The plaintiffs—victims of the breach—alleged that their names, social security numbers, addresses, and other identifying information were stolen.[133] The district court dismissed the plaintiffs' claim for lack of standing.[134]

The D.C. Circuit began its standing analysis by reviewing Supreme Court precedent.[135] Referencing the Court's decision in *Clapper*, the D.C. Circuit found Article III standing based on a substantial risk that harm would befall the data-breach victims.[136]

Distinguishing the case before it from *Clapper*, the court emphasized that the cyber assailant already had the victims' PII.[137] The D.C. Circuit stressed that the plaintiffs' claimed injury, the substantial risk of future identity theft, rested on a far less attenuated chain of events

127. *See id.* ("OPM contends that . . . it is impossible under these circumstances to easily construct any kind of colorable theory that a desire to commit fraud motivated the OPM breaches.").

128. *See id.* at 57 ("[G]iven that espionage and identity theft are not mutually exclusive, the likely existence of an espionage-related motive hardly renders implausible Arnold Plaintiffs' claim that they face a substantial future risk of identity theft . . . as a result of the breaches.").

129. *See id.* at 59 ("Given the nature of the information stolen and the fact that several named Arnold Plaintiffs have already experienced some form of identity theft since the breaches, it is at least plausible that Arnold Plaintiffs run a substantial risk of falling victim to other such incidents in the future.").

130. *See* Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017).

131. *See id.* at 622.

132. *See id.* at 623.

133. *See id.*

134. *See id.*

135. *See id.* at 625.

136. *See id.* at 626 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).

137. *See id.* at 628 ("Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers . . . .").

than that of the plaintiffs in *Clapper*.[138] Referencing the Seventh Circuit, the court considered the reprehensible uses for which a hacker could use the victims' information, such as making fraudulent charges or stealing the victims' identities.[139] Accordingly, the D.C. Circuit determined that the plaintiffs had satisfied Article III's injury-in-fact requirement.[140]

2. The Seventh Circuit

In 2013, Neiman Marcus[141] was the target of a cyberattack.[142] Using malware,[143] cyber assailants stole credit card information belonging to Neiman Marcus's customers.[144] In December 2013, Neiman Marcus learned of fraudulent charges that had appeared on credit cards belonging to some of its customers.[145] In January 2014, Neiman Marcus announced that approximately 350,000 credit cards were exposed in the breach and that 9,200 of those cards had been used fraudulently.[146] After the announcement, several potential victims of the breach brought suit against Neiman Marcus.[147] However, holding that the plaintiffs lacked Article III standing, the district court granted Neiman Marcus's motion to dismiss.[148]

On appeal, the Seventh Circuit began its Article III standing analysis with the injury-in-fact requirement.[149] The plaintiffs alleged that they suffered both an increased risk of future fraudulent charges and an increased risk of future identity theft.[150]

Referencing the Supreme Court's decision in *Clapper*, the Seventh Circuit recognized that the substantial risk of future harm can satisfy

138. *See id.* at 629 ("No long sequence of uncertain contingencies involving multiple independent actors 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.").

139. *See id.* (citing Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015)).

140. *See Attias*, 865 F.3d at 629 ("[The] risk is much more substantial than the risk presented to the *Clapper* Court, and satisfies the requirement of an injury in fact.").

141. Neiman Marcus is a clothing retailer. *See* NEIMAN MARCUS, http://bit.ly/2Hsdq41 (last visited Jan. 18, 2020).

142. *See Remijas*, 794 F.3d at 689.

143. "'Malware' is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, ..." Robert Moir, *Defining Malware: FAQ*, MICROSOFT (Apr. 1, 2009), https://bit.ly/2GueAzg.

144. *See Remijas*, 794 F.3d at 689–90.

145. *See id.* at 690.

146. *See id.*

147. *See id.*

148. *See id.* at 691.

149. *See id.* at 692.

150. *See id.*

Article III's injury-in-fact requirement.[151] Distinguishing the plaintiffs' alleged injury from the highly speculative injury advanced by the plaintiffs in *Clapper*, the Seventh Circuit acknowledged that the plaintiffs' information had already been stolen.[152] The court averred, "[victims] should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing."[153] Requiring the plaintiffs to wait until an injury materializes strengthens the defendant's argument that it did not cause the plaintiffs' injury because the causal link between the breach and the injury attenuates with time.[154]

Rejecting Neiman Marcus's argument that the plaintiffs' claimed injuries were too speculative, the Seventh Circuit quipped, "why else would hackers break into a store's database and steal consumers' private information? Presumably, to make fraudulent charges or assume those consumers' identities."[155] The court held that the plaintiffs' alleged substantial risk of future identity theft and future fraudulent charges were sufficient to satisfy Article III's injury-in-fact requirement.[156]

3. The Sixth Circuit

In 2012, Nationwide Mutual Insurance Company ("Nationwide") was hacked.[157] Cyber attackers breached Nationwide's network[158] and prevailed in stealing more than one million customers' PII.[159] In response to the breach, Nationwide offered its customers one year of free credit monitoring.[160]

Alleging negligence, among other claims, the victims brought suit against Nationwide.[161] The plaintiffs argued that an illegal market exists

151. *See id.*

152. *See id.* at 693

153. *Id.*

154. *See Remijas*, 794 F.3d at 693 (quoting *In re* Adobe Sys., 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014)) ("Requiring the plaintiffs 'to wait for the threatened harm to materialize in order to sue' would create a different problem: '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.'").

155. *Id.*

156. *See id.* at 694.

157. *See* Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 663 Fed. App'x. 384, 385 (6th Cir., filed Sept. 12, 2016).

158. Nationwide's computer network housed its customers' personal data, including their names, social security numbers, driver's license numbers, and birth dates. *See id.* at 386.

159. *See id.*

160. *See id.*

161. Plaintiffs alleged claims for invasion of privacy, negligence, bailment, and violations of the Fair Credit Reporting Act; however, only the negligence claim is pertinent to this Comment. *See id.*

for sales of data like that stolen from Nationwide's database.[162] Further, the plaintiffs argued that the breach created an "imminent, immediate and continuing increased risk" that they would suffer from identity fraud.[163] The plaintiffs corroborated this argument by citing a report purporting to show that, in 2011, data-breach victims were 9.6-times more likely to experience identity fraud and that there was a "fraud incidence rate"[164] of 19.6%.[165] The plaintiffs additionally bolstered their claim of future injury by citing the hours and dollars spent by breach victims to mitigate the risk of injury stemming from the data breach.[166]

Notwithstanding the plaintiffs' argument, the district court failed to find that they established Article III standing.[167] Thereafter, the plaintiffs appealed to the Sixth Circuit.[168]

Beginning its Article III standing analysis with the injury-in-fact requirement, the Sixth Circuit referred to the Supreme Court's decision in *Spokeo*.[169] The court quoted *Spokeo*, stating, "injury is the 'first and foremost' of standing's three elements."[170] The Sixth Circuit recognized that, where the claimed injury is imminent, Supreme Court precedent permitted finding standing based on substantial risk.[171]

The court reasoned that there was little need to speculate where the plaintiffs' data had already been compromised.[172] The Sixth Circuit was persuaded by the fact that Nationwide offered identity-theft protection and credit monitoring to its customers for a year following the breach.[173] To the court, this illustrated the severity of risk that the plaintiffs faced.[174] The Sixth Circuit rejected an argument that the plaintiffs sought to manufacture standing by incurring costs to mitigate risk.[175] The court

162. *See id.* ("Plaintiffs allege that there is an illicit international market for stolen data, which is used to obtain identification, government benefits, employment, housing, medical services, financial services, and credit and debit cards.").

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

164. *See Lesson 3: Measures of Risk*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://bit.ly/34JchjW, (last visited Oct. 11, 2020) (explaining that incidence rate can be thought of as the number of new incidences of identity fraud during a specified time interval, divided by the population at the start of the time interval). Here, the population would be the individuals whose data was compromised in a breach. *See id.*

165. *Galaria*, 663 Fed. App'x. at 386.

166. *See id.*

167. *See id.* at 387.

168. *See id.*

169. *See id.* at 388.

170. *Id.* (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

171. *See id.* (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).

172. *See id.* ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints.").

173. *See id.*

174. *See id.*

175. *See Galaria*, 663 Fed. App'x. at 388.

explained, "[w]here plaintiffs already know that they have lost control of their data, it would be unreasonable to expect plaintiffs to wait for actual misuse . . . before taking steps to ensure their own personal and financial security."[176] Ultimately, the Sixth Circuit held that the plaintiffs had satisfied Article III's injury-in-fact requirement.[177]

While the D.C., Seventh, and Sixth Circuits found standing based on the increased risk of future identity theft, the Fourth Circuit disagreed.[178]

4. The Fourth Circuit

In 2013, a laptop belonging to the William Jennings Bryan Dorn Veterans Affairs Medical Center ("VAMC") was stolen.[179] The laptop contained the personal information of approximately 7,400 patients.[180] The information included patient names, birth dates, and the last four digits of the patients' social security numbers.[181] In response to losing the information, VAMC offered one year of credit monitoring to the data-breach victims.[182]

The plaintiffs brought suit against VAMC, alleging, among other claims, that they faced a "future substantial harm from identity theft and other misuse of their [p]ersonal [i]nformation."[183] Relying on the Supreme Court's decision in *Clapper*, the district court granted the defendant's motion to dismiss for lack of Article III standing.[184] The district court determined that the plaintiffs' alleged injuries were too speculative and "contingent on a chain of attenuated hypothetical events and actions by third parties independent of the defendants."[185] The plaintiffs appealed to the Fourth Circuit.

On appeal, the Fourth Circuit began its standing analysis by assessing whether the plaintiffs' alleged injuries of a heightened risk of future identity theft were sufficient to satisfy standing's injury-in-fact requirement.[186] Agreeing with the district court, the Fourth Circuit contrasted the case before it from *Galaria v. Nationwide Mutual*

176. *Id.*
177. *See id.* at 389 ("[T]hese costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing.").
178. *See supra* Sections II.D.1–3; *see also infra* Section II.D.4.
179. *See* Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).
180. *See id.* at 267.
181. *See id.*
182. *See id.*
183. *Id.*
184. *See id.* at 267–68.
185. *Id.* at 268 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 422 (2013)).
186. *See id.* at 273.

Insurance Co. and *Remijas v. Neiman Marcus Group, LLC*.[187] The court observed that, even after discovery, the plaintiffs failed to find that the exposed information had been exploited.[188] The Fourth Circuit reasoned that the plaintiffs' alleged injuries relied on an "attenuated chain of possibilities," analogous to the scenario rejected by the Supreme Court in *Clapper*.[189] The court determined that the plaintiffs' alleged injuries were too speculative, even for the pleading stage of litigation.[190]

The plaintiffs supported their injury claims by arguing that "33% of health-related data breaches result in identity theft."[191] The Fourth Circuit rejected this argument.[192] After applying *Clapper*'s substantial risk test, the Fourth Circuit determined that the plaintiffs failed to show a substantial risk sufficient for standing's injury-in-fact requirement.[193] Furthermore, the Fourth Circuit determined that costs associated with the plaintiffs' mitigative measures were insufficient to confer standing.[194]

Similarly, the Eighth Circuit in *Alleruzzo v. SuperValu, Inc.* failed to find standing based on the increased risk of identity theft.[195]

5. The Eighth Circuit

Between June 22 and July 17 of 2014, cyber assailants hacked the computer network that processes payments for 1,045 SuperValu[196] stores.[197] The cyber assailants installed malware on SuperValu's network

187. *Id.* at 274 (quoting Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 663 Fed. App'x. 384 (6th Cir., filed Sept. 12, 2016)) ("[H]ackers broke into Nationwide's computer network and stole the personal information of Plaintiffs and 1.1 million others."); *see also id.* (quoting Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015)) ("Why else would hackers break into a store's database and steal consumers' private information?").

188. *Id.*

189. *Beck*, 848 F.3d at 275. ("In both cases, we must assume that the thief targeted the stolen items for the personal information they contained. And in both cases, the thieves must then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities. This 'attenuated chain' cannot confer standing.").

190. *See id.* at 274.

191. *Id.* at 275.

192. *See id.* at 275–76.

193. *See id.* at 276 ("This statistic falls far short of establishing a 'substantial risk' of harm.").

194. *See id.* at 276–77 (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011)) ("Simply put, these self-imposed harms cannot confer standing. . . . 'Mitigation expenses do not qualify as actual injuries where the harm is not imminent.'"); *see also id.* at 277 ("[P]rophylactically spen[ding] money to ease fears of [speculative] future third-party criminality . . . is not sufficient to confer standing.").

195. Alleruzzo v. SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017).

196. SuperValu is a retailer of groceries. SUPERVALU, https://bit.ly/3nyviOq (last visited Oct. 11, 2020).

197. *See Alleruzzo*, 870 F.3d at 766.

and used it to obtain SuperValu's customers' information.[198] The information obtained included customer names, credit or debit card account numbers, card expiration dates, card verification value numbers, and personal identification numbers.[199] SuperValu was victim to another hack in August 2014.[200]

The plaintiffs represented a group of SuperValu customers who had purchased goods from SuperValu using credit or debit cards between June and September 2014.[201] The plaintiffs brought suit against SuperValu, alleging that their payment card information had been stolen, which subjected them "to an imminent and real possibility of identity theft."[202] They averred that they spent time monitoring their account information to determine if their payment card information was compromised in the hack.[203]

At the trial court level, SuperValu prevailed in having the plaintiffs' complaint dismissed for failure to allege an injury-in-fact.[204] The plaintiffs appealed to the Eighth Circuit, which began its standing inquiry with the alleged injury, the risk of future identity theft.[205]

Referencing the Supreme Court's *Clapper* decision, the Eighth Circuit held that a future injury could be sufficient to confer standing.[206] The court determined that the plaintiffs' complaint sufficiently alleged that the hackers stole the plaintiffs' payment card information.[207] However, the Eighth Circuit noted that only one plaintiff's payment card information was actually abused.[208] The court was persuaded by a U.S. Government Accountability Office (GAO) report that stated that payment card information, without additional PII, cannot ordinarily be used to open new accounts.[209] Referencing the same GAO report, the Eighth Circuit explained that the GAO's findings did not support the plaintiffs' allegations that SuperValu's breach created a substantial risk that they would suffer credit or debit fraud or identity theft.[210] The court

198. *See id.*
199. *See id.*
200. *See id.*
201. *See id.*
202. *Id.*
203. *See id.* at 767.
204. *See id.*
205. *See id.* at 768.
206. *See id.* at 769.
207. *See Alleruzzo*, 870 F.3d at 769.
208. *See id.* at 770 ("[S]etting aside Holmes, [who had suffered a fraudulent charge on his credit card,] plaintiffs sufficiently allege that their Card Information was stolen by hackers as a result of defendants' security practices, but not that it was misused.").
209. *See id.* (referencing 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 30 (June 2007)).
210. *See id.* at 771.

concluded its injury-in-fact analysis by addressing the plaintiffs' argument that they had incurred costs to mitigate the risk of identity theft and credit or debit card fraud.[211] Referencing *Clapper*, the Eighth Circuit declared that the plaintiffs' efforts to mitigate a "speculative threat" could not create an injury-in-fact.[212] Accordingly, the court affirmed the trial court's dismissal of the plaintiffs' claim, rejecting the alleged future injury.[213]

6. Summary of the Circuit Split

As noted by legal scholars, federal courts have struggled to apply Supreme Court precedent concerning future injury and Article III's injury-in-fact requirement to cases involving claims of a substantial risk of identity theft following a data breach.[214] Generally, the federal circuits that *have* found standing based on the increased risk of future identity theft have appreciated (1) the nature of the data lost,[215] (2) the fact that said data could be put to nefarious uses,[216] (3) the fact that, in some instances, the responsible party had provided credit monitoring services to the victims,[217] and (4) the fact that, in some instances, fraud had already occurred.[218] Conversely, the federal circuits that *have not* found standing have determined either that the chain of events necessary for the identity theft to materialize was too attenuated to confer standing[219] or that, absent evidence of actual data misuse, the risk was too speculative.[220]

---

211. *See id.*

212. *See id.*

213. *See id.* at 771–72.

214. *See* Nathaniel Truitt, Note, *A Chance to Stand: Why "Loss-of-Chance" Should Replace the "Certainly Impending" Framework for Data Breach Cases*, 46 N. KY. L. REV. 22, 26 (2019) ("Unfortunately, it remains unclear how *Clapper* and *Spokeo* apply to data breach cases, and as a result, courts have inconsistently applied these holdings."); Hopkins, *supra* note 10, at 430 ("While Remijas and the affected Neiman Marcus customers successfully brought their claims in federal court and ultimately reached a settlement, had the case been filed in another circuit, the result could be different."); Martecchini, *supra* note 32, at 1483 ("Following the Court's own uncertainty in *Clapper* as to the appropriate imminence standard, a number of district courts have reached contrasting conclusions regarding the viability of standing based on increased risk in data-breach cases.").

215. *See* Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42, 56 (D.C. Cir. 2019).

216. *See* Attias v. CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015).

217. *See* Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 663 Fed. App'x. 384, 388 (6th Cir., filed Sept. 12, 2016).

218. *See Am. Fed'n of Gov't Emps.*, 928 F.3d at 56.

219. *See* Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017).

220. *See* Alleruzzo v. SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017).

Cyber assailants are compromising consumer records containing PII in malicious data breaches at unprecedented levels.[221] While the courts have been inconsistent in providing relief to data-breach victims, legislators have sought to enact statutes to protect consumers.[222]

E. Examining Existing Data-Privacy Law

The European Union and several states have responded to the demand for more robust data-privacy legislation.[223] Enacted by the European Union in 2016, the General Data Protection Regulation ("GDPR") is one of the most robust data-privacy laws in the world.[224] Similarly, in 2018, California legislators enacted the California Consumer Privacy Act of 2018 ("CCPA"), the most comprehensive state legislation on the issue of data privacy.[225]

1. The General Data Protection Regulation

The GDPR was enacted to "[protect] fundamental rights and freedoms of [people] and in particular their right to the protection of personal data."[226] The GDPR applies to the "processing of personal data in the context of activities of an establishment . . . in the [European] Union, regardless of whether the processing takes place in the Union or not."[227] The GDPR applies to virtually any establishment in the European Union that processes personal data.[228] The GDPR broadly defines "personal data" as any information that can directly or indirectly identify a person, including: "a name, an identification number, location data, an online identifier or to one or more facts specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[229] The GDPR defines "processing of personal data" broadly as any operation performed on personal data, including collection, storage, transmission, and destruction.[230]

---

221. *See supra* Section I.A.

222. *See infra* Sections II.E.1–2.

223. *See* Gregory S. Gaglione, Jr., Comment, *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity in America*, 67 BUFFALO L. REV. 1133, 1188 (2019).

224. *See id.*

225. *See id.*

226. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 1 (EU).

227. *Id.* art. 3.

228. *See* Alice Marini et al., *Comparing Privacy Laws: GDPR v. CCPA*, ONETRUST DATAGUIDANCE & FUTURE OF PRIVACY FORUM, Nov. 2018, at 1, 7.

229. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 4 (EU).

230. *See id.*

Substantively, the GDPR identifies several personal-data rights belonging to consumers, including: (1) the right to be informed about the use of personal data, (2) the right to access personal data, (3) the right to rectification of inaccurate personal data, (4) the right to the erasure of personal data, (5) the right to restrict processing of personal data, (6) the right to receive personal data in a portable format, (7) the right to reject to the processing of personal data, and (8) the right to not be subject to automated data processing.[231] To assure that these rights are protected, the GDPR requires that institutions subject to its protocols appoint a "data protection officer" to, among other duties, monitor compliance with the GDPR.[232]

In the event of a data breach, the GDPR mandates that the breached institution notify the appropriate supervisory authority within 72 hours of becoming aware of the breach.[233] Notification must disclose: (1) the approximate number of compromised records, (2) the likely consequences of the data breach, and (3) the measures taken by the breached institution to address the data breach.[234]

Significantly, the GDPR provides for judicial remedies for persons whose rights under the GDPR have been compromised due to noncompliance with its provisions.[235] In addition to a private right of action, the GDPR prescribes administrative fines for noncompliance.[236] The amount of administrative fines depends on the facts of each case, but significant consideration is given to: (1) intentional or negligent actions leading to infringement, (2) actions taken to mitigate damage, (3) categories of data affected, and (4) the nature, significance, and length of the infringement.[237] Violations of a person's rights, as described above, will subject the noncompliant institution to administrative fines up to €20 million[238] or, in the context of a parent-subsidiary relationship, "up to 4% of the total worldwide annual turnover of the preceding financial year," whichever is higher.[239] The threat of private action for noncompliance and the substantial administrative fines that liable establishments face encourage compliance with the GDPR's provisions.[240]

---

231. *See id.* arts. 12, 15–18, 20–22.

232. *See id.* art. 39.

233. *See id.* art. 33.

234. *See id.*

235. *See id.* art. 79.

236. *See id.* art. 83.

237. *See id.*

238. This represents $24,619,990.45. *See Currency Calculator with Live Exchange Rate*, CALCULATOR.NET, http://bit.ly/2uTygXp (last visited Jan. 6, 2021). The conversion is based on the January 6, 2021 exchange rate from openexchangerates.org.

239. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 83 (EU).

240. *See* Gaglione, *supra* note 223, at 1191.

2. The California Consumer Privacy Act of 2018

Enacted in the wake of the GDPR, the California Consumer Privacy Act ("CCPA") mirrors the GDPR while retaining notable distinctions.[241]

Beginning with scope, the CCPA applies only to California residents.[242] Further, the CCPA applies only to for-profit businesses that conduct business in California and collect consumers' personal information or have consumers' data collected on its behalf.[243] Lastly, the business must: (1) have a gross revenue exceeding $25 million, (2) annually buy, receive, or sell the personal information of 50,000 or more consumers, or (3) derive 50% or more of its annual revenue from selling consumers' personal information.[244] Recall, on the other hand, that the GDPR applies to all people and all establishments in the European Union that process personal data.[245] Indeed, the CCPA is decidedly narrower in scope than the GDPR.

Like the GDPR, the CCPA recognizes several personal-data rights. Specifically, the CCPA recognizes: (1) the right to the erasure of personal data, (2) the right to be informed about the use of personal data, (3) the right to opt out of certain uses of personal data, (4) the right to access personal data, (5) the right to not be discriminated against due to an invocation of a right, and (6) the right to receive personal data in a portable format.[246]

Despite the CCPA's robust protections, it does not contain a post-breach notification requirement.[247] Instead, the California legislature elected to maintain an existing post-breach disclosure statute, in lieu of creating a new disclosure regime.[248] Unlike the GDPR, the California notification statute does not provide a clear-cut timeframe for when notification must be provided.[249] Rather, the notification statute demands only that "the disclosure . . . be made in the most expedient time possible and without unreasonable delay."[250]

Like the GDPR, the CCPA provides a private right of action for certain data-breach victims.[251] Unlike the GDPR, which provides a

241. *See* Marini et al., *supra* note 228, at 5.
242. *See* CAL. CIV. CODE § 1798.140 (Deering 2018).
243. *See id.*
244. *See id.*
245. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 3 (EU).
246. *See* CIV. §§ 1798.100, .105, .120, .125, .130.
247. *See* Gaglione, *supra* note 223, at 1195.
248. *See* CIV. § 1798.82.
249. *See id.*
250. *Id.*
251. *Id.* § 1798.150.

private right of action for any violation of the GDPR,[252] the CCPA provides a private right of action when "nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of [the CCPA]."[253] Concerning remedies, the CCPA permits the greater of $750 in statutory damages or actual damages and injunctive relief.[254]

Finally, the CCPA authorizes the California Attorney General to impose civil penalties for violations of the CCPA.[255] Civil penalties under the CCPA are modest in comparison to those permitted by the GDPR[256] and range from $2,500 to $7,500.[257]

While the European Union and California have provided a potential roadmap for federal data-privacy legislation, federal legislators have yet to enact legislation on this front.[258] As a result, inconsistencies throughout U.S. courts leave consumers without a clear answer as to what their rights are after a data breach.[259]

III. ANALYSIS

As the risk of data breaches increases,[260] consumers deserve clarity as to the nature and extent of their personal-data rights. However, since the Supreme Court's decision in *Clapper*, courts have struggled to determine whether the increased risk of future identity theft is sufficient to confer standing.[261] Moreover, federal legislators have yet to enact comprehensive data-privacy legislation.[262] The Supreme Court and Congress, by providing clear legal rules and uniform federal legislation, respectively, could provide clarity to consumers.

252. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 79 (EU).

253. CIV. § 1798.150; *see* Marini et al., *supra* note 228, at 39.

254. *See* CIV. § 1798.150.

255. *See id.* § 1798.155.

256. *See supra* Section II.E.1.

257. *See* CIV. § 1798.155.

258. *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (Jan. 30, 2018), https://on.cfr.org/37uM3Ry ("The United States lacks a single, comprehensive federal law that regulates the collection and use of personal information.").

259. *See supra* Sections II.D.1–6.

260. *See supra* Section I.A.

261. *See supra* Sections II.D.1–6.

262. *See* O'Connor, *supra* note 258 ("The United States lacks a single, comprehensive federal law that regulates the collection and use of personal information.").

A. The Supreme Court

The Supreme Court must provide consumers with a clear-cut rule: the post-breach risk of future identity theft is either sufficient to establish Article III standing or it is not. This Comment encourages the Court to adopt a consumer-minded rule and recognize that the post-breach risk of identity theft is a sufficient injury-in-fact for Article III standing purposes.

The D.C., Sixth, and Seventh Circuits conducted a consumer-minded analysis and correctly held that the post-breach risk of future identity theft is sufficient for standing's injury-in-fact requirement.[263] These circuits properly considered the hyper-sensitive nature of the compromised data and the fact that said data was already in the hands of cyber assailants.[264] Moreover, as the Seventh Circuit reasoned in *Remijas*, by forcing victims to wait until identity theft occurs—increasing the temporal relationship between the breach and the ultimate harm—the defendants' argument that they did not cause the injury only strengthens.[265] As a result, victims then face trouble with Article III's second standing requirement, causality.[266]

The D.C., Sixth, and Seventh Circuit's consumer-minded injury-in-fact analysis better conforms to the Supreme Court's decisions in *Clapper* and *Spokeo*. Specifically, concerning injury-in-fact's imminence requirement, these circuits properly applied Justice Alito's language in *Clapper*.[267] To satisfy the imminence requirement, identity theft need not have already occurred; rather, a substantial risk of identity theft is sufficient.[268] Further, with regard to injury-in-fact's concreteness requirement, as Justice Alito indicated in *Spokeo*, the risk of real harm, such as the risk of identity theft, can satisfy this requirement.[269] Finally,

263. *See* Am. Fed'n of Gov't Emps. v. U.S. Office of Pers. Mgmt., 928 F.3d 42, 59 (D.C. Cir. 2019); Attias v. CareFirst, Inc., 865 F.3d 620, 629 (D.C. Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 663 Fed. App'x. 384, 389 (6th Cir., filed Sept. 12, 2016); Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015).

264. *See, e.g.*, *Remijas*, 794 F.3d at 693 ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is . . . to make fraudulent charges or assume those consumers' identities.").

265. *See id.*

266. *See supra* Section II.B.2.

267. *See, e.g.*, *Attias*, 865 F.3d at 626 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013)).

268. *See Clapper*, 568 U.S. at 414 n.5.

269. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

concerning injury-in-fact's particularization requirement,[270] objectors will struggle to find an injury more personal than the theft of one's PII.[271]

The Fourth and Eighth Circuit's business-minded reasoning is flawed.[272] These circuits have applied *Clapper*'s holding to deny data-breach victims relief.[273] This application is a poor fit in the context of post-breach harm. *Clapper* involved a speculated chain of events surrounding the surveillance of certain foreign communications.[274] But in the context of the post-breach harm discussed in this Comment, the PII is already in the hands of a cyber assailant.

Consumers need to know what their rights are when it comes to their PII, and survival of a motion to dismiss should not hinge on a particular circuit's pro-consumer or pro-business leaning.[275] To resolve this inconsistency, the Supreme Court should hold that the risk of future identity theft following a data breach is an injury-in-fact for standing purposes. Unfortunately, the Court has thus far refused to grant certiorari to cases centered on this issue.[276] The Court will likely maintain the existing *Clapper* and *Spokeo* precedent.[277] Accordingly, meaningful clarification will more likely come from Congress.

B. Congress Must Enact Comprehensive Data-Privacy Legislation

Congress should enact federal data-privacy legislation that provides data-breach victims with standing to bring suit against the responsible party. The General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") provide Congress with a sound starting point.[278]

Both the GDPR and the CCPA provide benefits to businesses and consumers. Both statutes provide consumers with several rights concerning their data, including the right to know how their data is being used[279] and the right to opt out of the sale of their data.[280] These rights

270. *See id.* at 1548 ("For an injury to be particularized, it must affect the plaintiff in a personal and individual way.").

271. *See supra* Section I.A.

272. *See supra* Sections II.D.4–5.

273. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017) (stating "[t]his 'attenuated chain' cannot confer standing").

274. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).

275. *See* Elizabeth Snell, *What the CareFirst Data Breach Decision Means for Healthcare*, XTELLIGENT HEALTHCARE MEDIA (Mar. 14, 2018), http://bit.ly/2OTvx79.

276. *See In re* Zappos.com, Inc., 888 F.3d 1020 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 1373 (2019); CareFirst, Inc. v. Attias, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

277. *See supra* Section II.C.

278. *See supra* Section II.E.

279. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 12 (EU); *see also* CAL. CIV. CODE § 1798.100.

provide consumers with more extensive knowledge of and control over how their data is leveraged. Businesses, too, will benefit.[281] By providing consumers with the right to opt out of their data being transferred, businesses will become more dependent on first-party data.[282] The greater accuracy and reliability of first-party data will help companies improve their marketing to consumers and their services.[283]

Additionally, both the GDPR and the CCPA provide data-breach victims with a private cause of action against the responsible party.[284] The private cause of action provides data-breach victims with a remedy in the event that a business's noncompliance results in the loss of the victim's PII and, in turn, provides businesses with an incentive to maintain compliance.[285] And aside from simply avoiding the costs of fines, one scholar maintains that compliance will save businesses money through reduced data-maintenance costs.[286]

Despite the GDPR's good intentions and benefits, some scholars have criticized it. One recurring criticism is the astronomical fines that the GDPR imposes on companies in the event of noncompliance.[287] As noted above, the GDPR permits fines of up to €20 million[288] and, given its far-reaching scope, implicates both small and large businesses.[289] In addition to "bankruptcy-inducing"[290] fines, one scholar estimated that it would cost more than $1 million for businesses to become compliant with the GDPR's procedural safeguards.[291]

Consumers cannot reasonably expect businesses to face the enormous penalties permitted by the GDPR and the high costs of GDPR compliance without either passing a portion of the costs on to

280. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 21 (EU); *see also* CIV. § 1798.120.

281. *See* Alison Divis, *How the CCPA Benefits Consumers and Business Owners*, PACIFIC DATA INTEGRATORS, http://bit.ly/2P0pcGX (last visited Oct. 7, 2020).

282. *See id.*

283. *See id.*

284. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 79 (EU); *see also* CIV. § 1798.150.

285. *See* Divis, *supra* note 281.

286. *See* Sneha Paul, *The Five Key Business Benefits of GDPR*, OPEN ACCESS GOV'T (Apr. 16, 2018), http://bit.ly/2HwaUtI.

287. *See* Larry Downes, *GDPR and the End of the Internet's Grand Bargain*, HARV. BUS. REV. (Apr. 9. 2018), http://bit.ly/2HtErUL; Daphne Keller, *The New, Worse 'Right to be Forgotten'*, POLITICO (Jan. 27, 2016), https://politi.co/325TTzR.

288. This represents $24,619,990.45. *Currency Calculator with Live Exchange Rate*, CALCULATOR.NET, http://bit.ly/2uTygXp (last visited Jan. 6, 2021). The conversion is based on the January 6, 2021 exchange rate from openexchangerates.org.

289. General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at arts. 3, 83 (EU).

290. Keller, *supra* note 287.

291. *See* Ray Schultz, *The Price of Compliance: Study Uncovers GDPR Costs*, MEDIAPOST (Oct. 26, 2017), http://bit.ly/2HulYax.

consumers[292] or changing their business models entirely.[293] Charging subscription fees for previously free services is one way of passing costs to consumers.[294] Consumers may encounter "tiered pricing," where certain content is available for free, while other content is hidden behind a paywall.[295] Under current business models, businesses use personal information to provide tailored-fit search results and recommendations, thus improving the consumer experience.[296] Businesses, in turn, may use this personal information as a revenue stream.[297] This quid pro quo has been referred to as "the Internet's Grand Bargain," and it has "been the fuel of digital growth for over two decades."[298] Given the GDPR's large penalties for noncompliance and high costs of implementation, businesses may shift away from this bargain, which could adversely affect the consumer product.

The CCPA has also been subject to criticism.[299] Like the GDPR, compliance with the CCPA will cost subjected businesses an appreciable amount of time and money.[300] These costs will likely be passed to the consumer in one form or another, such as by increased cost of use or a decreased service quality.[301]

Additionally, the depth of personal information covered by the CCPA has been criticized.[302] While obvious personal information, such as a person's name, birthdate, and social security number, is protected by the CCPA, the CCPA also extends to "inferences drawn [from personal information] . . . to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[303]

Congress is unlikely to go as far as the European Union, recognizing data privacy as a fundamental right,[304] or California,

292. *See* Niam Yaraghi, *A Case Against the General Data Protection Regulation*, BROOKINGS INST. (June 11, 2018), https://brook.gs/37yItWz.

293. *See* Downes, *supra* note 287.

294. *See* Yaraghi, *supra* note 292.

295. *See* Downes, *supra* note 287.

296. *See id.*

297. *See* Yaraghi, *supra* note 292.

298. Downes, *supra* note 287.

299. *See* Mike Masnick, *Yes, Privacy Is Important, But California's New Privacy Bill Is an Unmitigated Disaster in the Making*, TECHDIRT (July 9, 2018, 10:44 AM), http://bit.ly/2u1L7WX.

300. *See* Sarah Meyer, *CCPA Compliance Poses Significant Challenges for U.S. Companies*, CPO MAG. (Oct. 29, 2018), http://bit.ly/38t6pMd.

301. *See* Yaraghi, *supra* note 292.

302. *See* Masnick, *supra* note 299.

303. CAL. CIV. CODE § 1798.140 (Deering 2018).

304. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 1 (EU).

extending protections to virtually all personal information.[305] Further, given the exemptions that legislators often give to small businesses,[306] legislation as sweeping as the GDPR is unlikely.[307] Still, Congress can achieve a significant compromise that embraces many of the core principles of the GDPR and the CCPA.

C. Recommendation

Congress should enact legislation that provides data-breach victims with standing to sue the responsible party. Specifically, Congress should recognize that a violation of the proposed legislation that results in a PII-compromising data breach—and thus an increased risk of identity theft for the victims—constitutes an injury-in-fact for standing purposes.

Congress must enact federal legislation that narrowly defines the personal information and businesses covered by its provisions. The definition of personal information should include name, birthdate, social security number, driver's license number, and passport number. Further, federal legislation should mirror the CCPA and limit its reach only to those businesses most financially capable of implementing its safeguards.[308]

Further, federal legislation must recognize two consumer data rights: (1) the right to be informed by the business about how the business will use the consumer's data, and (2) the right to opt out of said uses. These rights promote transparency for consumers while permitting businesses to use the data once customers have given consent.

Additionally, the proposed legislation should mirror the GDPR by including a strict, 72-hour notification requirement once a company detects a data breach.[309] Where a consumer has entrusted their personal information to a business, a business should not be permitted to wait until it is financially favorable for them to disclose the breach to consumers.[310]

---

305. *See* CIV. § 1798.140.

306. *See, e.g.*, 26 U.S.C. § 4980H(a) (2018) (exempting employers with fewer than 50 employees from the Affordable Care Act's employer mandate); 29 U.S.C. § 2611(2)(B)(ii) (2018) (exempting certain employers with fewer than 50 employees from The Family Medical Leave Act of 1993); 42 U.S.C. § 12111(5)(A) (2018) (exempting employers with fewer than 15 employees from the Americans with Disabilities Act of 1990).

307. *See* Elizabeth Schulze, *The US Wants to Copy Europe's Strict Data Privacy Law – But Only Some of It*, CNBC (May 23, 2019, 1:16 AM), https://cnb.cx/3jMXJG3.

308. *See* CIV. § 1798.140.

309. *See* General Data Protection Regulation, Commission Regulation 2016/679, 2016 O.J. (L119), at art. 33 (EU).

310. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 690 (7th Cir. 2015) (observing that retailer Neiman Marcus waited until after the holiday season to notify consumers of the breach).

The proposed legislation should also include a private cause of action. Like the CCPA, the private cause of action should be limited to nonencrypted personal information lost due to a failure to comply with procedural safeguards.[311] Limiting the private right of action to nonencrypted personal information gives businesses an incentive to encrypt information while protecting businesses against liability for highly advanced breaches that overcome industry-recognized precautions.

The proposed legislation should, however, limit private remedies to statutory damages and attorney's fees. Statutory damages will compensate consumers for the time and money spent monitoring their information while protecting businesses from "bankruptcy-inducing" penalties.[312]

Finally, the proposed legislation should empower a federal agency to impose civil penalties on a noncompliant business where noncompliance has resulted in the compromise of personal information. While civil penalties should be substantial enough to deter subjected businesses from viewing noncompliance as a cost of business,[313] the civil penalties should not be of a magnitude that will force a business to close its doors permanently.

The GDPR and CCPA provide excellent starting points for federal legislation. However, neither statute is without valid criticism.[314] Accordingly, this Comment has sought to recommend a compromise that provides data-breach victims with standing to sue the responsible party while protecting businesses from door-closing consequences.

IV. CONCLUSION

The Supreme Court and Congress must provide consumers with clarity concerning their rights after a data breach that compromises their PII. Cyber assailants are stealing PII-containing consumer records at unprecedented levels.[315] Unfortunately, existing Supreme Court precedent on standing to sue for future harm has resulted in inconsistent applications at the federal trial and circuit court levels where data-breach

311. *See* CIV. § 1798.150.

312. *See* Keller, *supra* note 287.

313. Where penalties are insufficient to deter conduct, a business may elect to pay a penalty rather than change their conduct to comply with a regulation; that is, the business considers the penalty a cost of doing business. *See, e.g.*, Gregory M. Gilchrist, *The Expressive Cost of Corporate Immunity*, 64 HASTINGS L.J. 1, 51 (2012) ("Civil penalties lack the expression of condemnation inherent in criminal penalties. . . . The criminal penalty expresses opprobrium. The civil penalty expresses the cost of doing business. A criminal penalty can carry felon status. A civil penalty is little more than a price tag.").

314. *See supra* Section III.B.

315. *See supra* Section I.A.

victims allege an increased risk of future identity theft.[316] Further, federal legislators have failed to enact comprehensive data-privacy legislation.[317]

The Supreme Court should adopt the consumer-friendly approach taken by the D.C., Sixth, and Seventh Circuits and hold that the risk of future identity theft is sufficient for Article III's injury-in-fact requirement.[318] As the Seventh Circuit averred in *Remijas*, data-breach victims should not have to wait until hackers have stolen their identity to bring suit against the responsible party.[319]

Because the Supreme Court is unlikely to grant certiorari to parties raising the issue, Congress should enact federal data-privacy legislation that provides data-breach victims standing to sue noncompliant businesses. Congress should look to the General Data Protection Regulation and the California Consumer Privacy Act for guidance while striving to achieve a compromise that benefits consumers and protects businesses.[320]

316. *See supra* Sections II.D.1–6.

317. *See* O'Connor, *supra* note 258.

318. *See supra* Section III.A.

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

320. *See supra* Section III.C.