STANDING UP FOR THE LITTLE GUY: ESTABLISHING THAT INCREASED RISK OF FUTURE HARM IS ACTUAL HARM FOR DEMONSTRATING STANDING IN DATA BREACH CASES

ABSTRACT

Modern technology has changed the world for the better. As a result of technological advances, the world is more connected than ever through social media; medical treatment is more effective than ever through a vast network of treatment systems, centers, and specialists; monetary exchanges are more convenient through virtual and mobile payment systems; and information is more accessible to the masses through digital document storage formats. These modern advances all rely on personal data to function. For example, social media platforms require personal demographical data, medical systems require personal medical data, and mobile payment systems require financial data. Unfortunately, this data does not always remain in these systems—all too often these systems are breached by bad actors.

This Note discusses the current struggle faced by many victims of data breaches to establish standing in court to sue the parties they entrusted to protect their personal information. A current split exists between the various circuits of the United States Courts of Appeals. Some circuits allow victims to have standing as a result of their data being stolen, while other circuits require a higher showing of harmful data use before allowing standing. This Note breaks down this complex circuit split. It further calls on the United States Supreme Court to mend the split by setting certain standard rules which would more effectively aid victims in their pursuit of restitution and greater data protection without overburdening companies whose systems and services rely on massive data access.

TABLE OF CONTENTS

I. INTRODUCTION

In order to ensure the separation of powers between the executive, legislative, and judicial branches of the United States federal government, the jurisdiction of the federal courts has been limited to only "cases" and "controversies."[1] The concept of "judicial standing" arises from this limitation and sets the standards for determining what constitutes a case or controversy justiciable by the federal courts.[2] "To have standing in federal court, a plaintiff must show (1) that the challenged conduct has caused the plaintiff actual injury, and (2) that the interest sought to be protected is within the zone of interests meant to be regulated by the statutory or constitutional guarantee in question."[3]

With the rise of big data storage, and therefore big data breaches, circuit courts have struggled with how to apply the requirement of actual injury to the standing analysis.[4] In a simple tort case, it is clear and intuitive that a battered plaintiff whose arm is broken has suffered actual harm and can file suit. But what if a plaintiff's personal information is stolen—is there actual harm if the data has not yet been used to the plaintiff's detriment? Circuit courts currently disagree over how to handle this type of increasingly prevalent situation.[5]

1. Lujan v. Defs. of Wildlife, 504 U.S. 555, 559 (1992).
2. *Id.* at 559–60.
3. *Standing*, BLACK'S LAW DICTIONARY (11th ed. 2019).
4. *See* Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) (citing varying laws across circuits).
5. *Id.*

Part II of this Note discusses the origins of judicial standing, why it exists, and how the doctrine is currently understood today.[6] Part III explains how the current interpretation of standing conflicts with the growing issue of data breaches and how this conflict has led to a split among the various circuit courts.[7] Part IV proposes a modern solution which applies a tiered approach where standing can be established in data breach cases based on breach alone for certain crucial personal information.[8] Part V concludes the analysis of the issue.[9]

II. THE HISTORY OF STANDING, THE MODERN ELEMENTS OF STANDING, AND THE CURRENT VIEW OF ACTUAL HARM

A. *The Origin of Standing as a Restriction on Federal Court Jurisdiction*

A federal judiciary with the general power to adjudicate and interpret matters of law would be an overbearing power over the other two branches of the federal government, thus breaking down the separation of powers.[10] As a result, the U.S. Constitution imposed a cases and controversies limit on the federal courts.[11] However, what exactly amounts to a case or controversy has been largely left to interpretation by the federal courts—meaning the federal courts have over time limited their own ability to hear certain cases.[12]

6. *See infra* Part II.

7. *See infra* Part III.

8. *See infra* Part IV.

9. *See infra* Part V.

10. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 559–60 (1992) (citing THE FEDERALIST NO. 48 (James Madison)).

11. U.S. CONST. art. III, § 2, cl. 1 ("The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority . . . to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State,—between Citizens of different States,—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.").

12. Andrew R. Grindstaff, Note, *Article III Standing, the Sword and the Shield: Resolving a Circuit Split in Favor of Data Breach Plaintiffs*, 29 WM. & MARY BILL RTS. J. 851, 853 (2021) ("Constraints on the federal judiciary's power to adjudicate cases are largely, if not entirely, self-imposed limitations. As part of establishing a judicial branch coequal to the executive and legislature, Article III of the Constitution provides two restrictions on the Court's authority to hear judicial matters. First, federal courts may only hear actual 'cases' or 'controversies' implicating U.S. laws or citizens. Second, aside from the Court's original jurisdiction, Congress may strip the Court of jurisdiction.").

The federal courts have over time set forth doctrines to limit the scope of what cases and controversies they can hear.[13] "The precursor to modern standing doctrine required litigants to identify an existing common law interest to bring suit, rather than simply allege some harm."[14] By the 1970s, this requirement had given way to an "injury in fact" standard to make room for claims arising from regulations outside of the common law.[15] An injury in fact has to be a personal injury though; it may not just be a generalized grievance affecting society at large.[16] In order to have standing, federal courts also later determined that plaintiffs must show their injury in fact is a result of the defendant's actions without any attenuation to the causal link.[17]

B. *The Elements of Standing Today and the Current View of Actual Harm*

During the 1990s, the U.S. Supreme Court clearly set forth all of the requirements of standing in the case *Lujan v. Defenders of Wildlif*e.[18] The plaintiff must (1) allege to have suffered or imminently will suffer an actual injury (injury requirement), (2) show the actual injury is proximately or fairly traceable to the defendant (causation requirement), and (3) show facts that demonstrate the relief they are entitled to will substantially eliminate or redress the injury (redressability requirement).[19] What is meant by "imminently will suffer" harm is something the federal courts have recently struggled with.[20] In 2008, Congress amended the Foreign Intelligence Surveillance Act (FISA) to govern electronic surveillance of foreign communications for intelligence purposes.[21] U.S. plaintiffs, who regularly

13. *Id.*

14. *Id.* at 854.

15. *See id.*

16. *See* United States v. Richardson, 418 U.S. 166, 179–80 (1974) (holding a taxpayer does not have standing to challenge a statute regulating a federal agency's accounting and reporting procedures because generalized grievances that are common to all members of the public do not create standing; these issues are to be handled by the other branches and the political process at large).

17. *See* Allen v. Wright, 468 U.S. 737, 757–59 (1984) (finding no causal link between the Internal Revenue Service (IRS) allowing tax-exempt status for private schools that segregated against African Americans and the stigma the segregation created against African American students because it was not clear that the segregation would stop if the tax-exempt status was taken away).

18. *See* 504 U.S. 555, 560–61, 567–68 (1992) (holding threats to endangered species did not cause harm to the plaintiffs specifically and therefore ruling in the plaintiff's favor would not do anything to eliminate or redress the proposed harm).

19. *Id.* at 560–61.

20. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).

21. *Id.* at 404.

communicated internationally, sued claiming their communications would potentially be under surveillance.[22] The Supreme Court held that the fear of potential future surveillance and harm did not confer standing; instead the injury must be certainly impending, not merely objectively and reasonably likely.[23] The Supreme Court settled on this approach because it was unclear whether or not the plaintiff's communications would ever be targeted.[24] This issue of determining imminence is what has led to the current data breach circuit split.[25]

III. THE DISAGREEMENT OVER ACTUAL HARM IN DATA BREACH CASES: THE CURRENT CIRCUIT SPLIT

The Supreme Court's holding in *Clapper v. Amnesty International USA*—that plaintiffs cannot establish actual harm for standing purposes for possible future harm unless they show that the harm is certainly impending—has caused contention among the various circuit courts in cases related to data breaches.[26] This is especially the case considering later actions taken by the Supreme Court suggest that a "substantial risk" of future harm may also be a sufficient showing to establish standing.[27] Currently, the First, Second, Third, Fourth, and Eighth Circuits have not allowed a showing of actual harm based on potential future harm from data breaches, while the Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits have allowed actual harm to be shown based on potential future harm from data breaches.[28]

A. *Breaking Down the Split: Circuits Which Have Not Found Standing*

In *Katz v. Pershing, LLC*, in the First Circuit, a plaintiff on behalf of a class sued Pershing, LLC claiming that her private information, such as her Social

22. *Id.* at 406–07.

23. *Id.* at 410.

24. *Id.* at 411–12.

25. *See* Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) ("The Sixth, Seventh, and Ninth Circuits have all recognized, at the pleading stage that plaintiffs can establish an injury-in-fact based on [the] threatened injury . . . . By contrast, the First and Third Circuits have rejected such allegations.").

26. *See Clapper*, 568 U.S. at 410; Devin Urness, Note, *The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution*, 73 VAND. L. REV. 1517, 1538–40 (2020).

27. Urness, *supra* note 26, at 1524.

28. *See id.* at 1531–32; Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012); Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

Security number, had been left vulnerable to third parties due to Pershing's inadequate data protection practices.[29] The First Circuit found that since no breach of the plaintiff's data had been shown, no actual harm existed and therefore no standing could be established.[30]

In *Whalen v. Michaels Stores, Inc.*, in the Second Circuit, plaintiff Mary Jane Whalen brought suit against Michaels Stores after Michaels suffered a data breach which exposed customer credit card information, including Whalen's information.[31] Because Whalen did not allege any use of her credit card information incurred fraudulent charges, the Second Circuit found no actual harm and therefore no standing.[32]

In *Reilly v. Ceridian Corp.*, in the Third Circuit, plaintiffs filed a complaint on behalf of themselves and others alleging an increased risk of identity theft after Ceridian suffered from a data breach.[33] The breach contained personal and financial data, although it was unclear if the data was breached in a way that it could actually be read, copied, and understood.[34] The court concluded the allegations of hypothetical and future harm were too speculative and therefore not enough to show actual harm and standing.[35]

In *Beck v. McDonald*, in the Fourth Circuit, the plaintiffs, on behalf of a class, were veterans who sued after a data breach exposed their personal information.[36] The data breach occurred after a laptop was lost or stolen at the Veteran Affairs Medical Center containing the vital personal information of around 7,400 patients.[37] The Fourth Circuit held any risk of future harm from the breach to be too speculative and therefore not imminent.[38] The court stressed that no plaintiff found evidence of misuse or even showed evidence that the thief of the laptop had the intention of accessing their information.[39]

In *In re SuperValu, Inc.*, in the Eighth Circuit, 16 plaintiff customers sued SuperValu, Inc. after hackers were able to steal customer credit card information

29. *Katz*, 672 F.3d at 69–70.
30. *Id.* at 79.
31. 689 F. App'x 89, 89–90 (2d Cir. 2017).
32. *Id.* at 90–91.
33. 664 F.3d 38, 40 (3d Cir. 2011).
34. *Id.*
35. *Id.* at 42.
36. 848 F.3d 262, 266–67 (4th Cir. 2017).
37. *Id.* at 267.
38. *Id.*
39. *Id.* at 274.

via malware on multiple occasions.[40] Considering that the hackers likely did not have access to Social Security numbers, or other identifying information to be used in conjunction with the credit card information, the Eighth Circuit found it was not plausible that the breached information would ever be used to the plaintiffs' detriment.[41] Therefore, given these facts, there was no certain impending harm nor substantial risk of future harm from the data breach.[42]

All of these circuits on this side of the split, which found no standing, seemed to take a narrow approach to the concept of actual harm and standing in data breach cases.[43] The general rule is plaintiffs must still show some usage of their data or at least some definite intention to use the data.[44] This intention is often determined by showing that usage of the plaintiff's data was the motivation for the breach in the first place.[45]

B. *Breaking Down the Split: Circuits Which Have Found Standing*

In *Galaria v. Nationwide Mutual Insurance Co.*, in the Sixth Circuit, plaintiffs brought a class action after hackers breached the Nationwide Insurance network and stole personal information including Social Security numbers and drivers' license numbers.[46] Plaintiffs claimed Nationwide violated the Fair Credit Reporting Act by not having adequate data protection procedures.[47] Plaintiffs emphasized that there is a market for this information and that the information will therefore be used to steal their identities.[48] The Sixth Circuit found that even though it may not be "literally certain" the data will be used to the plaintiffs' detriment, it is not reasonable to require the plaintiffs to wait for the detriment to actually occur.[49] This will help plaintiffs mitigate the cost of credit-monitoring.[50]

40. Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc.), 870 F.3d 763, 766 (8th Cir. 2017).

41. *Id.* at 770–71.

42. *Id.* at 771.

43. *See* Kimberly Fasking, Comment, Beck v. McDonald*: The Waiting Game—Is an Increased Risk of Future Identity Theft an Injury-in-Fact for Article III Standing?*, 41 AM. J. TRIAL ADVOC. 387, 401–02 (2017).

44. *See id.*

45. *Id.* at 402–03.

46. 663 F. App'x 384, 386 (6th Cir. 2016).

47. *Id.*

48. *Id.*

49. *Id.* at 388.

50. *Id.* at 388–89.

In *Remijas v. Neiman Marcus Group, LLC*, in the Seventh Circuit, plaintiffs filed a class action against Neiman Marcus Group after the store suffered from a data breach in which customer credit card information was stolen.[51] The plaintiffs alleged current harm of:

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[52]

They also asserted imminent harm of "an increased risk of future fraudulent charges and greater susceptibility to identity theft."[53] The Seventh Circuit found actual harm from future, likely harm because hackers only stole the information to use the information to the plaintiffs' detriment.[54] The court noted that the causation was too attenuated because it did not allow the plaintiffs to have standing at the present and it would be easier for the defendants to have a claim in the future once the data is actually used.[55]

In *In re Zappos.com, Inc.*, in the Ninth Circuit, hackers stole the personal and credit card information of millions of Zappos customers.[56] Plaintiffs sued on behalf of a class citing an increased potential for identity theft.[57] The court ruled in favor of the plaintiffs, finding credit card information to be sensitive enough information to establish a risk of future identity theft.[58]

In *Resnick v. AvMed, Inc.*, in the Eleventh Circuit, plaintiffs, representing a class, sued AvMed after two laptop computers containing sensitive customer information were stolen from the AvMed office.[59] The plaintiffs argued the breach

51. 794 F.3d 688, 689–90 (7th Cir. 2015).

52. *Id.* at 692.

53. *Id.*

54. *Id.* at 693.

55. *Id.*

56. Stevens v. Zappos.com, Inc. (*In re* Zappos.com, Inc.), 888 F.3d 1020, 1023 (9th Cir. 2018).

57. *Id.*

58. *Id.* at 1027 (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding plaintiffs established actual harm and standing when a laptop containing sensitive personal information including Social Security numbers was stolen as there was a risk their identities would be stolen)).

59. 693 F.3d 1317, 1322 (11th Cir. 2012).

of the data did cause actual harm to the plaintiffs and that the harm was a result of AvMed allowing the laptops to be stolen.[60]

In *Attias v. CareFirst, Inc.*, in the D.C. Circuit, the information of customers was stolen from CareFirst, Inc. in a cyberattack.[61] The plaintiffs sued CareFirst on the grounds that the hackers would use their personal information to steal their identities.[62] The court, referring to the Seventh Circuit's decision in *Remijas*, sided with the plaintiffs and found actual harm and standing because there was no other reason why the personal information in this case had been stolen other than to eventually use it to the detriment of the plaintiffs.[63]

All of the circuits on this side of the split, which found standing, seem to take an expanded approach to the concept of actual harm and standing in data breach cases.[64] The general rule is once data is stolen, it is plausible to establish actual harm from substantial risk of future injury as a result of the data breach because that is why hackers hack—to eventually make use of the victims' identities.[65] There is no need to make the victims wait until the actual harm happens. Based on the facts of the cases on this side of the circuit split, factors to consider to move the needle from a plausibility of establishing harm to actually establishing harm include "(1) the presence of intent to specifically take the breached data, (2) the type of data released, and (3) the misuse of *any* of the data accessed during a breach."[66]

C. *Points of Contention and of Common Ground Between Both Sides of the Circuit Split*

Points of contention between the sides of the circuit split have arisen in three major ways as circuit courts have handled data breach cases: they consist of (1) hardware theft, (2) data hacking, and (3) mitigation efforts.[67]

When it comes to hardware theft, the circuits with an expanded approach to standing typically find that "[w]hen hardware is stolen, if that hardware contain[ed] information that would make future identity theft and fraud possible,

60. *Id.* at 1329–30.

61. 865 F.3d 620, 622–23 (D.C. Cir. 2017).

62. *Id.* at 623.

63. *Id.* at 628–29 (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015)).

64. *See, e.g.*, *Remijas*, 794 F.3d at 693–96.

65. Fasking, *supra* note 43, at 400.

66. Urness, *supra* note 26, at 1525–26.

67. Fasking, *supra* note 43, at 399–401.

the courts in the majority have held that it is enough to confer standing."[68] This concept is illustrated well in the *Resnick* case as the computers in that case contained unencrypted data, and the computers were deliberately taken for the purpose of accessing their contents.[69]

In comparison, "some courts in the [narrow view of standing] have based their rationale simply on an analysis of the likelihood of whether the thieves sought personally identifying information."[70] Courts stress it can be unclear whether or not laptops containing sensitive information are actually stolen in order to access their contents; many of these laptops have great value as equipment.[71] It is plausible that once the thieves find the sensitive information, they use it to steal identities; however, it is also likely they do not.[72] The court very clearly utilized this approach in *Beck*.[73]

In situations of data hacking, the circuits with an expanded approach to standing typically find that when personal information is targeted in a data hack, the intention to do future harm is clearly demonstrated; there are really no other benefits of a data hack.[74] The courts in *Galaria* and *Remijas* found no other compelling reason why the hackers would go through the effort to take the information if they were not either going to use the data themselves or sell it to another party who would then use the data to the detriment of the plaintiffs.[75]

Alternatively, "the courts [with the narrow view] are reluctant to find injury-in-fact for the purpose of Article III standing. These courts find the potential future misuse of the data leans too far toward 'speculative' to qualify as an imminent injury, such as in *Reilly v. Ceridian Corp*."[76] In *Reilly*, without any proof that the hackers could actually understand the data they stole, without any showing that the data would be enough to steal the plaintiffs' identities, and without any clearer intent to steal the plaintiffs' identities, the court found it was only hypothetical that

68. *Id.* at 399.

69. Resnick v. AvMed, Inc., 693 F.3d 1317, 1322, 1329–30 (11th Cir. 2012).

70. Fasking, *supra* note 43, at 402.

71. *Id.* at 402–03.

72. *See id.* at 403.

73. *See* Beck v. McDonald, 848 F.3d 262, 274–76 (4th Cir. 2017).

74. Fasking, *supra* note 43, at 400.

75. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388–89 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 692–93 (7th Cir. 2015).

76. Fasking, *supra* note 43, at 403–04 (referencing Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011)).

the plaintiffs would suffer harm; therefore, the harm was not imminent enough to constitute actual harm nor to confer standing.[77]

Once plaintiffs become aware their data has been stolen, most take mitigation efforts through practices such as credit monitoring; these practices cost money and take time.[78] Circuits with an expanded view of standing in data breach cases do not find actual harm through mitigation efforts alone; however, mitigation efforts do provide support for showing actual harm in the aggregate when combined with other factors such as the type of data stolen and the intention of the thief.[79]

In circuits with a narrow view, mitigation costs, such as credit monitoring in an attempt to avoid identity theft, do not provide support for actual harm.[80] The courts find that mitigation efforts taken and costs incurred are only based on mere speculation of harm—similar to security cameras being installed as protection against a potential robbery.[81] Fear alone is not enough to show that actual harm has occurred.[82]

IV. MENDING THE CIRCUIT SPLIT AND PROPOSING A SOLUTION THAT FITS THE MODERN WORLD

A. *A Clear and Universal Approach to Data Breach Standing That Holds Companies Accountable Is Crucial in Modern Society*

As a matter of policy, a coherent approach to data breach standing that maximizes the number of victims who can hold businesses accountable for poor data protection practices is preferable in today's digital world. This is because instances of stolen consumer data are more prevalent than ever.[83] The vast prevalence of stolen data is the result of a perfect storm of factors present in today's society.[84]

77. *Reilly*, 664 F.3d at 42–43.

78. *See* Fasking, *supra* note 43, at 395.

79. *See id.* at 401.

80. *Id.* at 404–05.

81. *See id.*

82. *See id.* (referencing *Reilly*, 664 F.3d at 46).

83. Chuck Brooks, *Alarming Cybersecurity Stats: What You Need to Know for 2021*, FORBES (Mar. 2, 2021, 7:15 PM), https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=41e9c6d58d3d [https://perma.cc/9ENJ-NWWU].

84. *See id.*

First, new machine learning techniques, coupled with new innovations such as 5G and artificial intelligence, make data hacking more effective and rewarding; greater interactions between hacker groups and hostile state actors also have this effect on hacking.[85] The more effective and rewarding hacking becomes, the greater incentives there are for bad actors to engage in the activity.[86] An example of this is the recent SolarWinds cyberattack in which 18,000 customers of SolarWinds installed malware added to the company's software by foreign, Russian-sponsored, hacker groups.[87] The malware allowed the hackers to access the customers' sensitive data for months undetected.[88]

Second, there are more potential victims than ever before.[89] "The number of Internet connected devices is expected to increase from 31 billion in 2020 to 35 billion in 2021 and 75 billion in 2025."[90] This surge in internet usage has resulted in one-fifth of all Americans falling victim to some level of data breach.[91] The data lost in these breaches is most often sensitive and personal data, as around two-thirds of all Americans have online accounts with companies which contain health, financial, and other personal identification information.[92] For example, in 2021, Kroger suffered a data breach resulting in 1,474,284 customer records being breached.[93] The records contained vital information, including, "[n]ames, contact information, Social Security numbers, insurance claim information, prescription information, and some medical history information."[94]

85. *See id.*

86. *See id.*

87. *See* Isabella Jibilian & Katie Canales, *The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal*, BUS. INSIDER, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 [https://perma.cc/RZJ7-BQDX] (Apr. 15, 2021, 12:25 PM) (describing SolarWinds as a major U.S. information technology company providing IT systems to other companies for their large-scale data management).

88. *Id.*

89. *See* Brooks, *supra* note 83.

90. *Id.*

91. *Id.*

92. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity: Americans' Experiences with Data Security*, PEW RSCH. CTR. (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/ [https://perma.cc/J9AR-WXWS].

93. Steve Alder, *Largest Healthcare Data Breaches of 2021*, THE HIPPA J. (Dec. 30, 2021), https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/ (stating that a total of 44,993,618 healthcare records were exposed or stolen in 2021).

94. *Id.*

Third, companies as a whole are not currently taking adequate preventative action to protect their consumer data from falling victim to hackers in this increasingly populated and hostile digital world.[95] "Nearly 80 [percent] of senior IT and IT security leaders believe their organizations lack sufficient protection against cyberattacks . . . ."[96]As a result, an alarming amount of Americans do not trust companies with their private data—Americans do not think their personal information is secure enough and are not content with the government's attempts thus far to protect their data.[97]

Because of the growing number of hackers, the increasing damage caused by data breaches, and the inadequacy of current consumer data protections, victims of data breaches must be able to hold as many companies as possible accountable in the courts.[98] Doing so should financially incentivize companies to take greater action to improve their cybersecurity practices.

B. *A Tiered Approach to Data Breach Standing Best Holds Companies Accountable Without Overburdening the Court System*

While policy considerations demand that victims of data breaches are able to swiftly bring forth their claims, the historical purpose of standing must not be ignored. Standing exists to limit the docket to cases and controversies established, in part, through actual injury indicated by a substantial risk of future harm.[99] Therefore, a solution to the circuit split, which allows too much litigation, is no solution at all—a balance must be met that broadens the scope of substantial risk enough to let the worst data breach cases in upon breach alone, while also barring lesser cases unless a higher standard is met. This can be accomplished through a tiered approach.[100]

Currently, the Sixth, Seventh, Ninth, Eleventh, and D.C. Circuits, which embody the expanded view of standing in which substantial risk and actual injury are established through breach alone, tend to base their decisions on the intentions

95. *See* Brooks, *supra* note 83.

96. *Id.*

97. *See* Matt O'Brien, *Americans Have Little Trust in Online Security: AP-NORC Poll*, U.S. NEWS & WORLD REP. (Sept. 16, 2021, 9:01 AM), https://www.usnews.com/news/business/articles/2021-09-16/americans-have-little-trust-in-online-security-ap-norc-poll.

98. *See* Brooks, *supra* note 83.

99. *See* Urness, *supra* note 26, at 1524.

100. *See* Grindstaff, *supra* note 12, at 874–76.

of the hackers.[101] This is best illustrated in the *Attias* case from the D.C. Circuit.[102] Meanwhile, the First, Second, Third, Fourth, and Eighth Circuits, which embody the narrow view of standing in which substantial risk and actual injury are not established through breach alone, tend to base their decisions on the type and variety of data stolen, as well as the accessibility of data stolen.[103] This is best illustrated in the *Beck* and *Supervalu* cases.[104]

Circuits with the expanded view find substantial risk of future harm by claiming that hackers would not steal data without intending to use it to the victims' detriment.[105] In effect, this allows most claims into court immediately.[106] Circuits with the narrow view counter this by claiming that just because hackers intend to use stolen data to the detriment of the victims and steal the data for that purpose, it does not mean the hackers obtained enough of the data or can understand enough of the data to do any harm.[107] In effect, this allows few claims into court immediately.[108]

The approach to standing in data breach cases that the Supreme Court should adopt to mend this split is to find a middle ground between the circuit split by creating tiers of data and applying different requirements of standing to each tier.[109] The high tier consists of the most sensitive data, including Social Security numbers, private health records, and financial information (such as credit card and banking numbers).[110] The low tier consists of all other personal data (such as home and email addresses, birthdays, names, and telephone numbers).[111]

In instances when high-tier data is stolen in a breach, this Note proposes that the expanded view of standing approach be implemented.[112] A Social Security number is crucial enough that after a breach alone there could be a substantial risk

101. *See, e.g.*, Attias v. CareFirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017); Urness, *supra* note 26, at 1531–32.

102. *See Attias*, 865 F.3d at 620.

103. *See, e.g.*, Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc.), 870 F.3d 763 (8th Cir. 2017).

104. *See, e.g.*, *Beck*, 848 F.3d at 276; *In re SuperValu, Inc.*, 870 F.3d at 766, 770–71.

105. *See Attias*, 865 F.3d at 628–29.

106. *See id.*

107. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 42–43 (3d Cir. 2011).

108. *See, e.g.*, *Beck*, 848 F.3d at 277–78; *Reilly*, 664 F.3d at 46.

109. *See* Grindstaff, *supra* note 12, at 874–76.

110. *See id.* at 875.

111. *See id.* at 876.

112. *See id.* at 875; Attias v. CareFirst, Inc., 865 F.3d 620, 628–29 (D.C. Cir. 2017).

of future harm through identity theft.[113] However, the same cannot necessarily be said about other high-tier data.[114] Therefore, in order to establish standing through breach alone without a Social Security number being stolen, two categories of other high-tier data must be stolen to increase the substantial risk.[115] For example, both health records and credit card information will suffice.[116] If only one category of the data is stolen, the rule for low-tier data will be followed.[117]

In instances when low-tier data is stolen in a breach, this Note proposes that the narrow view of standing approach be implemented.[118] Given that personal information such as addresses, birthdays, and telephone numbers are more public, and therefore less crucial for identification purposes, mere breach will not be enough to show actual harm as it is not substantially certain hackers would be able to use such data to harm a victim in any notable way.[119]

This tiered approach to data breach standing, if implemented by the Supreme Court, gives victims who have had their most personal information stolen the opportunity to immediately establish standing so that they may hold companies accountable for their poor cybersecurity practices.[120] The approach also protects the docket of the courts by keeping lesser data breaches from establishing standing upon breach alone.[121] Lastly, the emphasis on types of data through tiers keeps the idea of substantial certainty at the forefront of the standing analysis.[122]

V. CONCLUSION

For years, circuit courts have been split over how exactly to handle standing in cases of data breach.[123] When victims have crucial data stolen, the data is often

113. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010).

114. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011).

115. *See* Grindstaff, *supra* note 12, at 875–76.

116. *See* Alleruzzo v. SuperValu, Inc. (*In re* SuperValu, Inc.), 870 F.3d 763, 770–71 (8th Cir. 2017).

117. *See, e.g.*, *Attias*, 865 F.3d at 626 (describing the proposed rule for low-tier data).

118. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 273–76 (4th Cir. 2017).

119. *See* Grindstaff, *supra* note 12, at 876.

120. *See id.* at 874–76.

121. *Id.* at 874–77.

122. *Id.* at 877.

123. *Compare Beck*, 848 F.3d at 262 (applying the narrow view of standing), *with* Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) (applying the broad view of standing).

not used in any damaging way for a significant period of time.[124] Courts see the need to hold companies liable for losing consumer data given the growing prevalence of data breaches; however, without the data actually being used yet, the very idea of establishing liability runs contrary to the traditional views of standing.[125] Some circuits have found standing by finding substantial risk of harm through the intentions of the data hackers, while other circuits are skeptical and find future injury merely hypothetical.[126] The tiered approach set forth in this Note proposes the Supreme Court adopt a method of categorizing data based on importance and modifying the requirements of standing accordingly.[127] Victims with more crucial data stolen will have an easier time getting into court, while other victims must be more patient.

*Cole M. Krueger**

124. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 42–43, 46 (3d Cir. 2011) (considering the imminence of the harm for standing).

125. *See supra* Parts II, III.

126. *Compare Beck*, 848 F.3d at 262 (applying the narrow view of standing), *with Attias*, 865 F.3d at 620 (applying the broad view of standing).

127. *See supra* Part IV.B.

* Cole M. Krueger obtained his J.D. from Drake University Law School in 2023. He obtained his M.B.A. from the Drake University Zimpleman College of Business in 2023. He received his B.B.A. (Business Analytics concentration) from the University of Iowa Tippie College of Business in 2020.