SPREADING A DIGITAL DISEASE: THE CIRCUIT SPLIT ON DATA BREACHES AND ITS EFFECTS ON THE HEALTH SECTOR

NICOLE B. PERKINS*

I. INTRODUCTION

In the last decade, hackers stole personal information from millions of Americans. A Pew survey found that 64 percent of Americans "have personally experienced a major data breach."[1] A data breach means that there is a loss, theft, or unauthorized access to someone's confidential personal information contained in electronic data.[2] State laws often describe data breach notification requirements, and these laws differ from state to state.[3] There is no singular body of law that regulates the security of private personal information at the federal level, and it is instead sector specific.[4] The typical data breach begins with customers, clients, or patients handing over sensitive information to an organization or corporation they trust.[5] This sensitive information can include a broad spectrum of data, including social security numbers, bank account information, home addresses, trade secrets, and even matters of national security.[6] The attacker will pick a target that he perceives to be "weak" or not secure. The attacker typically will either use a network-based attack where he hijacks the network the organization uses, or he will use a social attack which could include phishing tactics.[7]

A. The Issue: Data Breaches and the Health Sector

The health industry experiences more data breaches than any other sector, typically because of medical identity theft.[8] The healthcare field provides a

---

* J.D. Candidate, 2023, Indiana University Robert H. McKinney School of Law; B.A., 2020, University of Dayton.

1. Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RSCH. CTR. (Jan. 26, 2017), https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ [https://perma.cc/G9U2-VW9C].

2. Andrew Froelich et al., *Data Breach,* TECH TARGET (July 2022), https://searchsecurity.techtarget.com/definition/data-breach [https://perma.cc/J36U-Y7KC].

3. *Security Breach Notification Laws,* NAT'L CONF. OF STATE LEG. (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/WJ7P-8XQH].

4. *Id.*

5. *Data Breach,* TRENDMICRO, https://www.trendmicro.com/vinfo/us/security/definition/data-breach [https://perma.cc/6LWX-DH3H] (last visited Oct. 16, 2021).

6. *Id.*

7. *Id.*

8. *Data Breaches in the Healthcare Sector,* CTR. INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ [https://perma.cc/JJ7Z-XU9R] (last visited Oct. 16, 2021).

unique opportunity for hackers to obtain deeply personal information about an individual that would not otherwise be shared with credit card companies, banks, or even their employer. For this reason, medical identity theft is on the rise as the fastest growing white collar crime in America.[9] Medical identity theft occurs when a hacker misuses the victim's medical identity such as records, health insurance, or personal information to obtain medical care.[10] The high numbers for data breaches in hospitals could also be due in part to the well-defined, legally mandated reporting requirements of the Health Insurance Portability and Accountability Act ("HIPAA").[11] In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") which required the Department of Health and Human Services and Federal Trade Commission to create notification requirements, so victims of data breaches would be alerted of a potential breach of their medical records.[12] The data protection model set up by HIPAA and the updates to notification requirements provided by HITECH still did not entirely fix the issue of medical identity fraud. Unlike financial identity theft victims, medical identity theft victims have very few private remedies available, which is problematic in how valuable medical information is for criminals.[13]

Personal Health Information ("PHI") is more valuable on the black market than credit card credentials or regular Personally Identifiable Information ("PII").[14] Therefore, there is a higher incentive for cyber criminals to target medical databases.[15] Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 268,189,693 healthcare records,[16] which equates to more than 81.72 percent of the population of the United States.[17] In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around one per day.[18] In December 2020, that rate had doubled. The average number of medical breaches per day for 2020 was 1.76.[19]

Those who feel threatened by their PHI in the hands of hackers and criminals have often turned to their state laws for potential legal recourse. Because state

---

9. *Medical Identity Theft on the Rise,* PROVIDERTRUST (Oct. 5, 2017), https://www.providertrust.com/blog/medical-identity-theft-rise/ [https://perma.cc/NGN3-2YSA].

10. Pam Dixon, *Medical Identity Theft: The Information Crime that Can Kill You*, WORLD PRIV. F. 1, 7 (2006), https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/ [https://perma.cc/7DAP-LZP3].

11. *Data Breaches in the Healthcare Sector, supra* note 8.

12. Howard Burde, *The HITECH Act: An Overview,* 13 AM. MED. ASS'N J. ETHICS 172, 183 (2011).

13. Dixon, *supra* note 10.

14. *Data Breaches in the Healthcare Sector, supra* note 8.

15. *Id.*

16. *Healthcare Data Breach Statistics,* HIPAA J., https://www.hipaajournal.com/healthcare-data-breach-statistics/ [https://perma.cc/3NXG-4EQ5] (last visited Oct. 16, 2021).

17. *Id.*

18. *Id.*

19. *Id.*

laws drastically differ depending on which state the breach occurred, the results for victims of data breaches have proven to be inconsistent. For example, the Supreme Court of New York granted a motion to dismiss for failure to state a claim when plaintiffs attempted to sue North Shore Long Island Jewish Health Systems when their PHI was stolen.[20] The Supreme Court granted the motion to dismiss because an increased risk of future identity theft does not satisfy the injury-in-fact requirements for standing. In other states that have similar statutory language, the result has been different. The Supreme Court of Georgia held that patients alleged a legally cognizable injury for negligence claim when there was a data breach by a hacker known as "Dark Overlord."[21] In that case, the Court stated "presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[22] The Court went on to state that for this reason, the plaintiffs' claim should not have been dismissed for failure to allege a cognizable injury because the risk of a patient's misuse of his or her PHI is "imminent and substantial."[23]

Reports have indicated that victims of health care fraud and medical identity theft increasingly wish to pursue legal action. In 2018, "5.7% of data breaches publicly reported led to class action litigation . . . indicating a steady increase in class action litigation relative to the number of breaches."[24] Many plaintiffs turn to the federal system, only to run into similar roadblocks.

B. Roadmap

This Note first discusses in Section II the constitutional standard for standing, followed by the current Supreme Court precedent cases which clarify the standards for Article III standing, *Clapper v. Amnesty International* and *Spokeo, Inc. v. Robins.* Section III then discusses how the circuit courts have interpreted these cases and the divide among the circuits. Section IV narrows in on the healthcare circuit split, focusing on the Third and D.C. Circuits' cases, *Attius v. CareFirst* and *Beck v. McDonald*. Section V discusses the implications of such a circuit split and the potential dangers it may cause within the healthcare sector. Section VI rejects a common solution to the data breach standing issue, which is a proposition for federal legislation and cites the recently decided *TransUnion v. Ramirez* Supreme Court case. Section VII proposes a different solution, which is that the Supreme Court should create a narrow ruling about data breaches and standing and should first hear a case in the healthcare field. In the healthcare setting, plaintiffs should be able to have standing for potential future harms.

---

20. Abdale v. N. Shore Long Island Jewish Health Sys., Inc., 19 N.Y.S.3d 850, 860 (N.Y. Sup. Ct. 2015).

21. Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310, 311 (Ga. 2019).

22. *Id.* at 315.

23. *Id.* at 316.

24. David Zetoony et al., *Data Breach Litigation Report*, BRIAN CAVE LEIGHTON PAISNER L. 1, 2 (2019), https://www.bclplaw.com/images/content/1/6/v6/163774/2019-Litigation-Report.pdf [https://perma.cc/P4QT-GNNC].

This Note concludes with a warning that a blanket ruling on standing for data breaches could be potentially dangerous to small businesses who did not foresee litigation costs. This Note advocates for a narrowly tailored ruling to the healthcare sector which implements a balancing test. This balancing test would weigh the fact that the healthcare sector has suffered some of the largest security breaches in the country, while also considering that hospitals and healthcare facilities may follow up-to-date data breach protections. Additionally, this Note advocates for a narrow ruling tailored to the health care industry because it will also help frame the issue for future judicial decisions in other areas outside of the healthcare sector.

II. TURNING TO PRECEDENT

Although the Supreme Court has not addressed a data breach case specifically, the individual justices have debated for years about the constitutional interpretation of standing and when plaintiffs should be able to get past the pleading stage.

A. Constitutional Foundation and Early Case Law

Standing is the initial determination of whether or not a person who believes he or she has been wronged has grounds to sue based on the contextual understanding of Article III of the United States Constitution.[25] Article III, which governs federal courts, places a limit on the judiciary and dictates that federal courts can only hear "cases" and "controversies" that are "traditionally amenable to, and resolved by, the judicial process."[26]

The Supreme Court in *Lujan v. Defenders of Wildlife* decided that to sue in federal court, a plaintiff must establish an injury-in-fact to show an invasion of their protected interest; that is (a) concrete and particularized and (b) actual or imminent.[27] In *Lujan,* the case centered around the Endangered Species Act (ESA), which seeks to protect animals against threats to their continuing existence caused by man.[28] Section 7(a)(2) of the ESA requires each federal agency to consult with the United States Secretary of the Interior to ensure that any action authorized, funded, or carried out by the agency in question is not likely to jeopardize the continued existence of any endangered or threatened species of animals.[29] The ESA also states that any person can begin a civil suit on her own behalf to enjoin anyone, including governmental agencies from violating

---

25. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (*citing* Allen v. Wright, 468 U.S. 737, 751 (1984)) ("[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III.").

26. Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 102 (1998).

27. *Lujan*, 504 U.S. at 555.

28. *Standing Under the Supreme Court's Landmark Luhan v. Defenders of Wildlife Decision*, CON. LAW REP. (2018), https://constitutionallawreporter.com/2020/02/25/lujan-v-defenders-of-wildlife-decision/ [https://perma.cc/HUE2-JZW2].

29. *Lujan*, 504 U.S. at 558.

the ESA.[30] In 1978, the Secretaries promulgated a joint regulation stating that the ESA Section 7(a)(2) requirement will extend to federal actions in foreign countries.[31] However, in 1986, the regulation limited the geographic scope to the United States and the high seas.[32] Organizations dedicated to the protection of endangered animals and wildlife generally sued the Secretary of the Interior, Lujan, seeking a declaratory judgment that the new regulation is incorrect, and requested an injunction requiring the Secretary to restore the initial interpretation of the geographic scope.[33] The plaintiffs argued they were injured because a lack of consultation for governmental activities abroad increases the rate of extinction.[34] The Secretary moved to dismiss based on lack of standing.[35]

The Court held that a plaintiff may not litigate a generalized complaint against the government based on harm suffered equally by all citizens.[36] The Court famously stated, "an injury in fact is an invasion of a legally protected interest which is (a) concrete and particularized . . . and; (b) actual or imminent."[37] The Court also notably stated that the injury must be fairly traceable to the challenged action and not the result of the independent action of some third party.[38] *Lujan* is still considered the touchstone case for analyzing Article III standing. The subsequent Supreme Court opinions surrounding Article III standing attempt to clarify when plaintiffs have standing for future harms, which was not squarely addressed in *Lujan*.

B. Clapper*'s "Substantial Risk" and "Certainly Impending" Standards*

Clapper v. Amnesty International USA expanded upon the actual and imminent harm element of standing.[39] The plaintiffs in *Clapper* challenged 50 U.S.C. §1881a, an amendment of a provision of Foreign Intelligence Surveillance Court Amendments Act of 2008 ("FISA"), which authorized the United States government to conduct surveillance without probable cause on non-U.S. citizens who were outside the United States. Under this amendment, the government would be able to conduct surveillance without the usual requirements to obtain permission from the Court to intercept communications.[40] By shrinking the requirements under FISA, the government only needed to demonstrate that the surveillance they seek to intercept targets "persons reasonably believed to be located outside the United States" and seeks to "acquire foreign intelligence

30. *Id.* at 572.
31. *Id.*
32. *Id.* at 560.
33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.* at 551.
37. *Id.*
38. *Id.* at 552.
39. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).
40. *Id.* at 404.

information."[41]

The plaintiffs in this case were attorneys and human rights, labor, legal, and media organizations whose work allegedly required them to engage in confidential, and sometimes privileged communications with colleagues, clients, sources, and other individuals who are located outside of the United States.[42] The plaintiffs brought suit seeking a declaratory ruling that this portion of FISA was unconstitutional.[43] The plaintiffs claimed there was an "objectively reasonable likelihood" of injury that the plaintiffs' communications would be recorded under FISA. Alternatively, the plaintiffs claimed that given the risk of surveillance, they had a present injury because such risk required them to spend significant funds to ensure that their communications were kept confidential.[44]

The Court ruled that the plaintiffs did not have standing.[45] Justice Alito, writing for the majority, articulated the "certainly impending" standard, stating that the plaintiffs' "speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impeding or is fairly traceable to FISA."[46] The case was dismissed because an injury for standing purposes must be "certainly impending," and because the plaintiffs could not satisfy the constitutional requirement to bring suit. However, in a footnote of the opinion, the Court stated that plaintiffs do not need to uniformly prove that it is "literally certain that the harms they identify will come about.[47] In some instances, the Court admitted they have found standing based on a "substantial risk" that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[48] The Court then goes onto say that the plaintiffs in this case missed the mark on both the "substantial risk" standard and the "clearly impending" requirement in light of the "attenuated chain of inferences necessary to find harm here."[49] Justice Alito then addressed the plaintiff's alternative argument, that they established standing on the measures they have taken to avoid FISA surveillance. He states, "Respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[50]

While *Clapper* is factually unrelated to a data breach, *Clapper* has proven to be the touchstone case used by corporations when victims allege harm from a breach of their information due to a hacking of the corporation's systems. In many ways, *Clapper* has "tightened" the standing test, making it more difficult for plaintiffs to litigate their issues in court.

---

41. *Id.* at 404-05.
42. *Id.* at 409.
43. *Id.*
44. *Id.* at 406-507.
45. *Id.* at 414.
46. *Id.*
47. *Id.* at 414-15 n.5.
48. *Id.*
49. *Id.*
50. *Id.* at 416.

In *Clapper*'s dissent, Justice Breyer took issue with the "certainly impeding" standard, perhaps predicting that entities sued for failing to protect consumer data would assert this as a defense. He stated that plaintiffs will struggle to make the connection between the danger they believe they are in, like a breach of information, with a certainly impending harm.[51] He states "[T]he word 'certainly' in the phrase 'certainly impending' does not refer to absolute certainty. As our case law demonstrates, what the Constitution requires is something more akin to 'reasonable probability' or 'high probability.'[52] According to Justice Breyer, the plaintiffs' claims here were not based on "attenuated chain of inferences" but rather on facts providing that interception was highly likely.[53] The plaintiffs here reasoned that the government's past behavior demonstrated an interest in seeking the information that the plaintiffs would engage in. The allegations were not based on an unreasonable fear but on facts proving that interception was likely.[54]

C. Spokeo *and Further Confusion with "Concrete Injury" Standard*

The decision in *Clapper* caused much confusion among the circuit courts. As a result of this confusion, the Supreme Court heard *Spokeo, Inc. v. Robins,* an appeal out of the Ninth Circuit. The plaintiff, Robins, filed a class action lawsuit against Spokeo alleging that information pulled on him through Spokeo search engine was inaccurate, thus, violating the Fair Credit Reporting Act's procedures for requiring accuracy as a reporting agency.[55] Spokeo provides personal information about individuals to a variety of users, including employers researching potential employees.[56] Spokeo collects information on individuals from a multitude of databases. This information includes phone numbers, addresses, marital status, age, occupation, shopping preferences, and even musical preferences.[57] Robins asserted that his Spokeo profile caused him to suffer actual harm to his employment, because the inaccurate reporting of his alleged graduate degree and children made him seem overqualified and unlikely to relocate because of family obligations.[58]

The Court re-examined the injury in fact requirement of standing and found that the injury suffered must be "concrete and particularized."[59] The Court held that , the plaintiff only alleged an intangible harm, which was not concrete nor particularized, thus, the plaintiff had no standing.[60] The Court reasoned that although there was a violation of a procedural right granted by a statute, the

---

51. *Id.* at 441.
52. *Id.*
53. *Id.*
54. *Id.* at 444.
55. Spokeo, Inc. v. Robbins, 578 U.S. 330, 334 (2016).
56. *Id.*
57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.* at 1544.

plaintiff cannot satisfy the demands of Article III by alleging a bare procedural violation. The plaintiff experienced no "concrete harm."[61] The Court did not take this opportunity to define what constitutes a "concrete" injury, nor did it declare whether a risk of future harm was enough to constitute an injury-in-fact, for purposes of establishing Article III standing, specifically the element of imminence. The Court stated that although an abstract injury is not a concrete one, an intangible injury can be sufficient, if it is fairly traceable to the defendant's actions and the court can redress the injury.[62]

Although the Court did not explicitly identify whether an increased risk of future harm is enough to satisfy the element of imminence, it stated that a statutory right created by Congress cannot automatically give an individual the right to sue.[63] The violation of a statutory right must be combined with a concrete injury.

Unfortunately, *Spokeo* did nothing to resolve the circuit split resulting from *Clapper*. The *Spokeo* decision did not address the question of whether a data breach without any financial loss constitutes a concrete injury for Article III standing. Circuits remain split on whether the risk of future harm is sufficient to establish Article III standing, and now they are wrestling with exactly how *Spokeo* applies to allegations of an increased risk of identity theft following a data breach.

III. THE CIRCUIT SPLIT REGARDING DATA BREACHES

Federal circuits over the past few years have wrestled with *Clapper* and *Spokeo* interpretations, and the question of whether plaintiffs in a data breach class action can establish standing, if they only allege a heightened "risk of future harm" still lingers. The Third, Sixth, Seventh, Ninth, and D.C. circuits have generally found standing, while the First, Second, Fourth, Fifth, and Eighth circuits have generally found no standing where plaintiff only alleges a heightened "risk of future harm."[64] The Third and D.C. circuits addressed that question specifically within the healthcare sector and found standing, where the Fourth and Fifth circuits addressed the same question within the healthcare sector and found no standing.[65] The arguments on either side are driven by considerations for businesses, policy, and what constitutes standing.

A. Plaintiffs Have Standing

Due to the unclear standing standard set out in *Clapper* and reinforced in

---

61. *Id.* at 1550.

62. *Id.* at 1547.

63. *Id.*

64. Jason C. Gavejian & Maya Atrakchi, *The Circuit Split Continues: 11th Circuit Weighs in on Standing in Data Breach Litigation*, JACKSON LEWIS (Mar. 23, 2021), https://www.workplaceprivacyreport.com/2021/03/articles/data-breach-notification/the-circuit-split-continues-11th-circuit-weighs-in-on-standing-in-data-breach-litigation/ [https://perma.cc/V4AT-RHFT].

65. *Id.*

Spokeo, circuit courts have struggled to determine whether future harm from a data breach would be sufficient to establish a "concrete injury." While the D.C., Sixth, Seventh, and Ninth circuits have allowed these claims to move forward with an alleged risk of future injury, the Second, Third, Fourth, and Eighth circuits have not. The Seventh, D.C., and Sixth Circuits have all found that, when personal information is stolen, plaintiffs have standing based on the risk of a future harm because, as stated by the D.C. Circuit, "at the very least, it is plausible to infer that [the thief] has both the intent and the ability to use that data for ill."[66] Additionally, because the facts of *Clapper* did not involve a data security breach, these courts are much more inclined to extend standing to victims of data breaches because this risk was perhaps unforeseen by the Justices in *Clapper.* Most courts concede that a financial harm or identity theft relating to a data breach is sufficient to satisfy the injury-in-fact component of standing.[67]

B. Plaintiffs Do Not Have Standing

Some circuits do not recognize these types of "injuries" as sufficient to constitute standing. For example, in *Reilly v. Ceridian Corp.*,[68] the Third Circuit found that where allegations of a future injury required speculation, injury was not sufficiently imminent for the purposes of standing.[69] *Reilly* perhaps set an example to future cases in finding that the alleged increased risk of future injury was entirely speculative because it depended upon the future actions of a third party.[70] Additionally, the court held that there was no evidence that the intrusion was malicious.[71] As for the healthcare industry, an important case which highlights a similar analysis as *Reilly,* is *Beck v. McDonald.* In *Beck,* the Fourth Circuit held that there was no injury where plaintiffs could not show that information contained on a stolen laptop was misused, or that the thief intended to misuse the information.[72] The analysis consistent among the circuits that find future harm insufficient to establish standing is that Article III standing is a higher threshold to meet than merely showing an increased risk of harm subject to a data breach.

IV. HEALTHCARE SPLIT

Because the healthcare sector experiences such a large percentage of the data breaches, focusing on the DC and Fourth Circuit's approach to standing and data breaches displays the need for a healthcare-specific ruling from the Supreme

---

66. Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017).

67. *See* Robert D. Fram et al., *Standing in Data Breach Cases: A Review of Recent Trends*, COVINGTON & BURLINGTON LLP (Nov. 9, 2015), http://www.bna.com/standing-data-breach-n57982063308/ [https://perma.cc/YK29-UF6J].

68. Reilly v. Ceridian Corp., 664 F.3d 38, 39 (3d Cir. 2011).

69. *Id.* at 42-43.

70. *Id.* at 45.

71. *Id.*

72. Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).

Court. There are two specific cases with opposite holdings that deal with the healthcare sector which highlight this discrepancy: *Attius v. CareFirst* and *Beck v. McDonald*.

A. Attias*'s Pro-Plaintiff Approach to Standing*

In *Attias v. CareFirst, Inc.*, CareFirst and its subsidiaries are a group of health insurance companies who provide health insurance to approximately one million customers in the District of Columbia, Maryland, and Virginia.[73] When customers purchased CareFirst's insurance policies, they handed over information about themselves including their names, birthdates, email addresses, social security numbers, and credit card information.[74] The companies stored this information on their servers. Allegedly, CareFirst failed to properly encrypt some of the data entrusted to its care.[75] Seven insureds subsequently filed a class action lawsuit against CareFirst.[76] The parties disagreed on whether the hackers were able to obtain the insureds' social security numbers, and CareFirst sought to dismiss the claims for lack of standing.[77] The plaintiffs argued that they suffered an increased risk of identity theft as a result of the data breach, but the district court found this theory of injury to be too speculative.[78]

The D.C. Circuit Court relied on *Clapper,* specifically footnote 5*,* to conclude that an "injury in fact" exists when there is a "substantial risk" that the injury will occur.[79] The Court distinguished the facts of *Attias* from *Clapper* by stating that unlike *Clapper,* the alleged injuries were not comprised of many links in a casual chain.[80] The Court in *Attias* stated that, in assuming all the allegations in the complaint were true (meaning social security numbers and credit card information were stolen), it was not too speculative to consider the plausible harms that plaintiffs could endure because, "at the very least, it is plausible to infer that [the thief] has both the intent and the ability to use that data for ill."[81] Therefore, the plaintiffs had standing. The Court referred to a 7th Circuit decision, *Remijas v. Neiman Marcus Grp.*, which held that it is plausible to infer that the individuals whose information was stolen had shown a substantial risk of harm from the data breach by allegations of future injury.[82] Therefore, the Court held that the allegation could survive a motion to dismiss for failure to state a claim. The Court in *Attias* specifically quoted the 7th Circuit in re-stating "Why else would hackers break into a . . . database and steal consumers' private information? Presumably,

---

73. Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017).
74. *Id.* at 623.
75. *Id.*
76. *Id.*
77. *Id.* at 622.
78. *Id.* at 624.
79. *Id.* at 626.
80. *Id.*
81. *Id.* at 627.
82. Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

the purpose of the hack is . . . to make fraudulent charges or assume those consumers' identities."[83] Moreover, the Court reasoned that the nature of the hack and the information stolen merited a finding that a "substantial risk" existed. The Court in *Attias* reasoned that the type of fraud that could occur that is unique to the healthcare industry. The Court stated that the combination of members' names, birth dates, email addresses, and subscriber ID numbers alone qualifies as material theft when taken in conjunction with the heightened risk of medical identify theft.[84] The Court states that medical identity theft occurs when a "fraudster impersonates the victim and obtains medical services in her name."[85] That sort of fraud leads to "inaccurate entries in [victims'] medical records" and "can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs."[86] The Court says that these portions of the complaint "would make up, at the very least, a plausible allegation that plaintiffs face a substantial risk of identity fraud, even if their social security numbers were never exposed to the data thief."[87] This argument is important because the court identifies the unique harm that is associated with medical fraud. This decision by the D.C. Circuit "amplifies the circuit split by strengthening the hand of potential class action litigants, and it may signal a potential turning of the tide on the issue of standing when the data breach involves intentional hacking."[88]

B. Beck *and The Hacker's Intent*

The Fourth Circuit did not find constitutional standing in *Beck v. McDonald* when a laptop with private information was stolen along with four boxes of pathology reports.[89] The laptop and reports were stolen from William Jennings Bryan Dorn Veterans Affairs Medical Center ("the VAMC") in Columbus, South Carolina.[90] The stolen laptop contained unencrypted personal information of roughly 74,000 patients and the missing boxes held information for over 2,000 patients.[91] The information stolen was very similar to the information that was compromised in *Attias*, including names, birth dates, the last four digits of social security numbers, descriptive traits of patients, and medical diagnoses.[92] The VAMC's own investigation concluded that the stolen

---

83. *Id.*

84. *Attias*, 865 F.3d at 627.

85. *Id.* at 628.

86. Id.

87. *Id.*

88. Edward R. McNicholas & Grady Nye*, D.C. Circuit Widens the Split on Standing in Data Breach Cases After Spokeo*, SIDLEY (Aug. 8, 2017), https://datamatters.sidley.com/d-c-circuit-widens-split-standing-data-breach-cases-spokeo [https://perma.cc/NV39-B8ZP].

89. Beck v. McDonald, 848 F.3d 262, 266 (4th Cir. 2017).

90. *Id.*

91. *Id.* at 267.

92. *Id.* at 268.

information resulted from VAMC's failure to follow proper procedures for maintaining personal information on encrypted computers.[93] The VAMC contacted its patients in accordance with South Carolina data breach notification requirements, and at least seventeen additional data breaches ensued due to failure to properly implement procedures to secure information.[94]

Richard Beck and Lakreishia Jeffrey, veterans who received treatment at the VAMC, filed a class action suit on behalf of the victims of the stolen personal information.[95] The plaintiffs sought relief under the Privacy Act of 1974 for the threat of "current and future substantial harm from identity theft and other misuse of their [p]ersonal [i]nformation,"[96] thus relying on *Clapper*.

The Court found that the theft of unencrypted laptops and pathology reports were too speculative to confer standing without proof that the thief acted for the purpose of obtaining personal information.[97] The Court held that there was no proof that the thief stole the laptop with the purpose of obtaining the personal information.[98] The Court in *Beck* determined that, in cases which found standing, the individual who stole personal information acted with the sole purpose of obtaining stolen personal information.[99] The Fourth Circuit distinguished the facts in *Beck* when it concluded that there was a deliberate targeting of personal information in other cases, and in doing so it relied upon factors. These factors included the sophistication of the hacking that took place, the lack of an alternative explanation for the hacking, and the fraudulent activity (such as identity theft and fraudulent charges) suffered by the plaintiffs.[100]

Additionally, the Court in *Beck* emphasized that, because the plaintiffs' stolen information was not used for fraudulent activity, from the time of the theft in 2014 to the time of the suit in 2017, there was no risk of "substantial harm."[101] While the hack in *Attias* also occurred in 2014, the D.C. Circuit reasoned that the stolen information still created a plausible "substantial risk" of harm, irrespective of the time that had passed without incident, such that the passage of time did not mitigate or negate the substantial risk.[102]

C. Effect of the Circuit Split within the Healthcare Sector

Attias and *Beck* demonstrate the divergence of analysis within the courts as to what constitutes a sufficient injury for victims of medical data breaches. The argument in *Beck*, that the injury in fact is not certainly impeding, largely

---

93. *Id.* at 276.
94. *Id.* at 268.
95. *Id.* at 267.
96. *Id.*
97. *Id.* at 273.
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.* at 275.
102. Attias v. CareFirst, Inc., 865 F.3d 620, 628 (D.C. Cir. 2017).

discounts the pertinent issue of stolen medical records in the hands of hackers or thieves. Cybersecurity firm Protenus, tracked 222 health care data hackings in 2018, and said that figure was up 25 percent since 2017.[103] The ambiguity among the circuits and the lack of guidance from the Supreme Court is spreading a digital disease among medical patients in the United States. While patients suffer from physical ailments and put their trust in their doctors and insurers, they are also unknowingly subjecting themselves to another danger: fraud and extortion.

V. FUTURE HARMS

If the circuit split persists, the healthcare field will become confused and frustrated, and the patients affected by data breaches will face long-term repercussions.

A. Issues with Medical Records Are Difficult to Resolve

According to a Federal Trade Commission consumer bulletin, medical identity theft is when someone uses your information to obtain a consultation with a doctor, purchase medical devices, submit false insurance claims, or obtain prescription drugs.[104] Gary Cantrell, head of investigations at the United States Department of Health and Human Services- Office of Inspector General said hackers tend to steal medical records because they are like "a treasure trove of all this information about you." They contain a patient's full name, address history, financial information, and social security number—which is enough information for hackers to take out a loan or set up a line of credit under patients' names.[105] The health care sector has relatively low security, so it is "easy" to get a large amount of data for medical fraud.[106] To put the value of medical records into perspective, social security numbers sell on the dark web for prices as low as $1, credit card information sells for around $110, but Experian reports full medical records sell for up to $1,000, and an entire database from a hospital in Georgia sold for $26,000.[107]

---

103. *What Hackers Actually Do with Your Stolen Medical Records,* ADVISORY BD. (Mar. 1, 2019, 10:00 AM), https://www.advisory.com/daily-briefing/2019/03/01/hackers [https://perma.cc/HSY8-S22Z].

104. Lisa Tomaszewski, *The Dangers of Medical Identity Theft*, PHYSICIAN'S WKLY. (Oct. 13. 2021), https://www.physiciansweekly.com/the-dangers-of-medical-identity-theft [https://perma.cc/8RKD-K36B].

105. *Hackers are Stealing Millions of Medical Records – and Selling Them on the Dark Web,* CBS NEWS (Feb. 14, 2019, 7:37 AM), https://www.cbsnews.com/video/hackers-are-stealing-sensitive-medical-records-and-selling-them-on-dark-web/ [https://perma.cc/VY2V-7YM7].

106. *What Hackers Actually Do with Your Stolen Medical Records, supra* note 92.

107. *Hackers are Stealing Millions of Medical Records – and Selling Them on the Dark Web*, *supra* note 106.

B. Credit Report Issues and Other Issues

It is not always certain when the information will be used. Hackers can keep the information for years before deciding to take action that would compromise the innocent party.[108]Buyers of medical information might use the information to create fake IDs to purchase medical equipment or drugs, or to file a false insurance claim.[109] Even after the hacker is caught, the hospital or insurance company that used this false information may still have the victim's medical information in the hacker's medical file.[110] Additionally, PHI, such as information regarding a sexually transmitted disease or terminal illness, could be used to extort or coerce someone.[111]

Many people have reported that they cannot get the charges "scrubbed" from the credit report until the next billing cycle, but by then the hacker would have already committed more medical fraud.[112] There have also been cases of innocent people being arrested because someone has stolen their medical identity and used it to purchase an overabundance of prescription drugs in their name.[113]

In 2004, Brandon Reagin, a young Marine, lost his wallet.[114] Months later, his mother called Reagin stating that local authorities are looking for him because of multiple car thefts.[115] Upon looking into the matter, Reagin realized someone was having multiple medical procedures under his name, and the bills added up to nearly $20,000.[116] Reagin attempted to dispute the charges on his credit report, but on the next billing cycle the charges appeared again.[117] As of 2019, Reagin still has not been able to undo all the damage caused by the hacker. The hospital that performed the procedures on the criminal still has the criminal's blood type under Reagin's name, which resulted in health insurance issues, and confusion among healthcare professionals who have performed procedures on Reagin himself.[118] Cybersecurity expert Gary Miliefsky, estimates it takes about "three seconds" to retrieve patient files off the dark web.[119]

---

108. *Id.*

109. Background on: Insurance Fraud, INS. INFO. INST., https://www.iii.org/article/background-on-insurance-fraud [https://perma.cc/5BGT-AF2M] (last updated Feb. 15, 2022).

110. *Hackers are Stealing Millions of Medical Records – and Selling Them on the Dark Web*, *supra* note 106.

111. Id.

112. *What Hackers Actually Do with Your Stolen Medical Records, supra* note 103.

113. Tomaszewski, *supra* note 104.

114. *Hackers are Stealing Millions of Medical Records – and Selling Them on the Dark Web*, *supra* note 103.

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

VI. FEDERAL LEGISLATION IS NOT THE ANSWER

Many observers and researchers of the circuit split advise for a piece of federal legislation that could potentially confer standing for victims of data breaches. This recommendation stems from a case decided by the Third Circuit, *In re Horizon Healthcare Services Inc. Data Breach Litigation.* This case relied on the Fair Credit Reporting Act ("FCRA") to confer standing. However, in July 2021, the Supreme Court took issue with statutory standing for alleged future harms in the case *TransUnion LLC v. Ramirez*.

A. Horizon Health Care*'s Successful Use of the FCRA*

In 2017, the Third Circuit case *In re Horizon Healthcare Services Inc. Data Breach Litigation*, was the result of two unencrypted laptops containing detailed personal information on approximately 839,000 clients were stolen from Horizon's headquarters.[120] The information on these laptops contained personal information and health information of clients and potential clients.[121] The named plaintiffs were among the members whose PHI had been stolen, but they did not allege that their personal information had been viewed or used by the thieves or other third parties.[122] In bringing the class action lawsuit, plaintiffs alleged, among other state claims, separate claims for willful and negligent violations of the FCRA, maintaining that Horizon was a consumer reporting agency under the Act.[123] The Third Circuit found standing for the plaintiffs under the FCRA, which is a body of legislation that attempts to protect consumer privacy and imposes requirements on consumer reporting agencies.[124] The Third Circuit clarified that this ruling did not contradict *Spokeo* because the plaintiffs alleged more than a "mere technical or procedural violation," but an "unauthorized dissemination of their own private information--the very injury that FCRA is intended to prevent."[125] The *Horizon Healthcare* decision provided another potential avenue—a violation of a statutory right—for plaintiffs in class action data breach lawsuits to obtain standing.[126] Many have proposed that there should be federal

---

120. *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 630 (3d Cir. 2017).

121. *Id.*

122. *Id.*

123. *Id.* at 631. *See also* Robert A. Stern, *The State of Article III Standing in the Third Circuit under Horizon Healthcare Services, Inc. Data Breach Litigation - And More*, MORRISON MAHONEY (Feb. 21, 2017), https://www.morrisonmahoney.com/blog/256-the-state-of-article-iii-standing-in-the-third-circuit-under-horizon-healthcare-services-inc-data-breach-litigation-and-more [https://perma.cc/Q39U-6ZGK].

124. *Id.* at 635.

125. *Id.* at 640.

126. Gregory N. Blasé et al., Third Circuit Moves Toward a Broader View of Standing in FCRA Data-Breach Class Action, K&L GATES (Jan. 30, 2017), http://www.klgates.com/third-circuit-moves-toward-a-broader-view-of-standing-in-fcra-data-breach-class-action-01-30-2017/ [https://perma.cc/X7B4-QEWA].

cybersecurity legislation, but that would pose a new unique set of issues.

B. The Recent Supreme Court Decision and What It Means for Plaintiffs Alleging Future Harms Under the FCRA

On June 25, 2021, the United States Supreme Court issued its decision in *TransUnion v. Ramirez,* which will have rippling effects on the theory that plaintiffs can sue for a statutory violation when it comes to data breach litigation. In *TransUnion,* Sergio Ramirez acted as a representative for a class-action lawsuit against credit report agency TransUnion.[127] Ramirez alleged that TransUnion willfully violated the FCRA by indicating on his credit report that his name appeared on a government list of individuals prohibited from conducting business in the U.S.[128] Ramirez had attempted to buy a car, but when the dealership ran a credit check, the credit report wrongfully indicated that Ramirez was on a list of suspected terrorists with whom U.S. companies are barred from doing business.[129] Ramirez followed up with TransUnion, who had provided the credit report, and TransUnion sent Ramirez two mailings indicating that his name was a "potential match" for two names on the Terrorist Watch List.[130] Ramirez claimed that those mailings did not comply with the Fair Credit Reporting Act.[131] The class members in *TransUnion* fell into two groups: (1) those whose potential status as a national security threat was shared with third parties, and (2) those who were merely flagged in TransUnion's internal records.[132] A jury in the U.S. District Court awarded over sixty-million dollars in damages to the class members.[133] On appeal, the Ninth Circuit affirmed the district court's judgment, but reduced the per-member punitive damage amount.[134] TransUnion argued that the case should not have been allowed to go forward as a class action because there was not a guarantee that each class member had suffered the same kind of injury required by the Constitution to be able to file suit.[135] TransUnion appealed to the Supreme Court of the United States.[136]

The Supreme Court held in *TransUnion* that consumer class action claims under the FCRA must allege the actual spread of misleading information to third parties to establish standing to assert a claim.[137] This decision supplements

---

127. TransUnion, LLC v. Ramirez, 141 S. Ct. 2190, 2200 (2021).

128. *Id.* at 2201.

129. *Id. See also* Amy Howe, *Court Limits Standing in Credit Reporting Lawsuit,* SCOTUSBLOG (Jun 15, 2021, 1:58 PM), https://www.scotusblog.com/2021/06/court-limits-standing-in-credit-reporting-lawsuit/ [https://perma.cc/8Q4D-JU3B].

130. *Id.* at 2201-02.

131. *Id.* at 2202.

132. *Id.*

133. *Id. See also* Howe, *supra* note 116.

134. *Id.*

135. *Id. See also* Howe, *supra* note 116.

136. *Id.*

137. *Id.* at 2201.

Spokeo, which further restricts the circumstances where a statutory violation can form the basis of a claim.[138] The majority opinion, written by Justice Kavanaugh, specifically rejected that the consumers in the class, whose information was not shared with third parties, had standing under the FCRA to assert a claim based upon a risk of future harm.[139] Justice Kavanaugh emphasized that the Constitution requires plaintiffs suing in federal court to have a "personal stake" in the case. The Court noted that, although Congress' views on what constitutes a concrete and particularized injury can be helpful, Article III is not satisfied merely because Congress created a statutory cause of action.[140] Justice Kavanaugh emphasized that "only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over that violation in federal court."[141] Absent analysis from the judiciary, Congress could potentially create opportunities for far too many lawsuits, thus flooding the courts. *TransUnion* further indicates that a statutory violation, like the one found in *Horizon*, will not be enough for future victims of healthcare data breaches to find legal recourse.

C. Why Federal Legislation Does Not Work in the Healthcare Context

Conferring statutory standing for victims of healthcare fraud or medical identity theft is unlikely to provide plaintiffs with a way to hold the health sector accountable. As *TransUnion* demonstrates, Article III requirements are a "hard floor," and Congress may not circumvent them entirely.[142] Congressional legislation may authorize litigation by conferring standing within Article III's confines. However, litigants are required to show "a distinct and palpable injury to [themselves]" that a court can remedy.[143] Congress may not direct federal courts to hear cases where Article III standing is not met. The fact that the Third Circuit found standing under the FCRA, and then the Supreme Court denied standing on similar grounds, demonstrates the need not for more federal legislation, but rather interpretation from the judiciary. Even further, "disagreements between Republicans and Democrats in Congress have blocked proposed federal legislation addressing data breach issues."[144] Even if there was federal legislation governing cybersecurity, it still would require a "collaboration between the legislature and the judiciary by requiring the judiciary to evaluate companies' compliance with cybersecurity policies mandated by the legislation."[145] In other words, regardless of whether there is federal legislation

---

138. *Id.* at 2204.

139. *Id.* at 2212.

140. *Id.* at 2204-05.

141. *Id.* at 2212.

142. Summers v. Earth Island Inst., 555 U.S. 488, 497 (2009).

143. Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91, 100 (1979).

144. Richard Cowan & Susan Cornwell, *Republicans Defend Grip on U.S. Congress as Trump Wins Presidency*, REUTERS (Nov. 8, 2016, 6:13 AM), http://www.reuters.com/article/us-usa-election-congress-idUSKBN13317Z [https://perma.cc/L9TT-EDUB].

145. Van Ha Le & Bianca Zamora, *The Price of a Data Breach*, 4 INFO. SYS. AUDIT &

or not, the Supreme Court would still need to guide the interpretation.

VII. THIS NOTE'S PROPOSED SOLUTION

This Section of this Note begins by advocating that the Supreme Court should take a data breach case involving a hospital or health insurance company because of the particularized harm the plaintiffs will likely have. This Section then provides the reasons why there should not be a universal rule on data breach standing, and why hospitals are vulnerable targets. To understand why the Supreme Court should evaluate standing in the health sector, it is important to recognize the harm in creating a generalized rule for all data breaches.

A. More Particularized Harm

Because medical identity theft is a particularized type of harm that could cause catastrophic damage, the future harm is more concrete and particularized, which would satisfy the standards set out in *Spokeo* and *Clapper.* Victims of a healthcare data breach have potential harms that are "certainly impending." The HIPAA Security Rule establishes national standards to protect individuals' electronic PHI that is created, received, used, or maintained by a covered entity.[146] The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[147] Because there is no private right of action under HIPAA, victims of a data breach in the healthcare sector have minimal opportunity for legal recourse.[148]

The FCRA option of legal recourse has proven to be dependent on a circuit court's interpretation of what is a mere procedural violation and what is a statutory violation, and the Supreme Court's most recent decision in *TransUnion* furthers the need for guidance from the Supreme Court as to the difficulties in data breaches.

B. Safety Precautions for Hospitals and Health Insurers

Most breached healthcare organizations that SecurityMetrics, a payment card industry data security standard company, has investigated did not have an incident response plan at the time of the breach.[149] A decision from the Supreme

---

CONTROL ASS'N J. 1, 14 (2018).

146. *Summary of the HIPAA Security Rule,* U.S. DEPT. HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [https://perma.cc/2YUW-CUDG] (last updated July 26, 2013).

147. *Id.*

148. Ryan Knox, *The 'P' is Not for Privacy: Preventing Private Enforcement of HIPAA*, PROC. N.Y.U. MOOT CT. BO. (April 22, 2019), https://proceedings.nyumootcourt.org/2019/04/the-p-is-not-for-privacy-preventing-private-enforcement-of-hipaa/ [https://perma.cc/DR63-HFA3].

149. Jen Stone, *How to Manage a Healthcare Data Breach*, SEC. METRICS, https://www.securitymetrics.com/blog/how-manage-healthcare-data-breach [https://perma.cc/8GJQ-TNVV] (last

Court that would find standing for victims of a healthcare data breach would signal to hospitals that they should be taking the same precautions as large corporations in the business sector do. Many state level privacy laws exist for businesses. In 2018, California adopted one of toughest privacy laws of any state with the Consumer Privacy Act. It introduced new obligations for businesses to disclose information about data collection and protections for consumers that include a right to delete personal information and a right to opt out of having their information sold.[150]

C. Universal Rule on Data Breaches Could Hurt Businesses

Given that it is typical for data breach class actions to involve tens of millions of plaintiffs, many corporations cannot withstand a financial blow of this magnitude.[151] If a minimal showing of injury-in-fact sufficiently establishes standing, corporations, large and small, will face immense liability, considering the frequency and severity of data breach class actions. Additionally, defendants in data breach class actions must notify affected consumers.[152] With an average notification cost of five dollars per class member, the aggregate amount becomes financially crippling.[153]

The Federal Trade Commission agrees that there is no such thing as perfect security and data breaches inevitably will happen.[154] Therefore, it is unreasonable to expect corporations to install an impenetrable fortress of data security.[155] If courts allow a mere increased risk of identity theft to satisfy the injury requirement, attempts to establish an impenetrable system are incentivized due to the impending class action liability. For this reason, there needs to be specific interpretations of who can bring suit against corporations, and the healthcare sector is a good place to start because of the high level of privacy concerns and the specific information that could potentially be released.

VIII. POTENTIAL HOLDING OF THE U.S. SUPREME COURT

The Supreme Court has had opportunities to address the "injury in fact" requirement of Article III standing, but failed to articulate a comprehensive standard that can be applied to future case law. This Note advocates for a balancing test that the Court can use as a tool to weigh the plaintiffs' potential future injuries against the preparedness of the hospital. Specifically, this

---

visited Oct. 16, 2021).

150. *Id.*

151. Ha Le & Zamora, *supra* note 145.

152. FED. R. CIV. P. 23(c)(2).

153. Ha Le & Zamora, *supra* note 145.

154. Jared Ho, *Corporate Boards: Don't Underestimate Your Role in Data Security Oversight,* FED. TRADE COMM'N. (Apr. 28, 2021, 9:29 AM), https://www.ftc.gov/news-events/blogs/business-blog/2021/04/corporate-boards-dont-underestimate-your-role-data-security [https://perma.cc/E859-5TVC].

155. *Id.*

balancing test will examine the demonstrable probability of negative consequences of an individual's PHI in the wrong hands with reasonability of protections instituted to prevent disclosure. This balancing test will provide an opportunity for the hospital or healthcare facility to assert as a defense that they were also a victim of hacking and that they did everything that they could to prevent a data breach. The factors within this balancing test would focus first on the plaintiffs themselves and will look at (A) the significance of the information stolen, and (B) the time frame in which the complaint was filed. The next factor will then look at the hospitals and examine (C) the reasonableness of the hospital's security maintenance. An overwhelming inclination toward one factor could outweigh a deficiency in another factor.

A. The Significance of the Information Stolen

HIPAA classifies all of a patient's PHI into eighteen different categories.[156] This Note advocates that for the first element of the balancing test the Court will examine whether the stolen information falls into any of these categories. Although this list is expansive and encompasses many kinds of data, HIPAA clarifies that any data that (1) does not identify the patient, or (2) is used or disclosed by a covered entity during the course of care, is not considered PHI.[157] This distinction is important because using this standard, there are cases where PHI may not have been leaked.

In *Khan v. Children's National Health System,* there was no evidence that the information in the breach had been misused or had even been accessed.[158] The hacker used phishing tactics to access the email accounts of certain employees at the hospital.[159] The hacker did not hack the electronic medical records system or some other centralized database of personal data, so it was nearly impossible to tell what information the hacker had access to.[160] The Court found that the plaintiff, Khan, lacked standing because the circumstances of the data breach did not clearly indicate that the hackers' purpose was to use the patients' personal data to engage in identity fraud.[161] Although this Note agrees with the holding of *Khan,* this Note advocates that the hackers' intent should not be the focus of the potential harm. To quote the Seventh Circuit in *Remijas,"*Why else would

---

156. Abi Tyas Tunggal, *What is Protected Health Information (PHI)?,* UPGUARD, https://www.upguard.com/blog/protected-health-information-phi [https://perma.cc/V8X2-XLDX] (last updated Aug. 25, 2021). The HIPAA categories are names, geographical identifiers smaller than a state, dates other than year related to a person, phone numbers, fax numbers, email addresses, social security numbers, medical record numbers, health plan beneficiary numbers, health plan beneficiary number, account numbers, license numbers, vehicle numbers, evidence identifiers, URLs, IP addresses, finger prints, full facial photos, and any other unique identifying number.

157. *Id.*

158. Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 527 (D. Md. 2016).

159. *Id.*

160. *Id.*

161. *Id.* at 532.

hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is . . . to make fraudulent charges or assume those consumers' identities."[162] The intent of the hacker is less important than the significance that the information has on the plaintiff. In *Khan,* the Court could have considered the lack of significant data the hackers had access to and still reach the same conclusion that the plaintiffs lacked standing.

By explicitly enumerating the type of data that is considered "significant," this factor of the balancing test will clarify *Clapper*'s "certainly impending" standard. In order to satisfy this factor, a plaintiff will have to identify a category that their stolen information falls under. If the plaintiff fails to do so, the harm cannot be said to be "certainly impending," so this factor within the balancing test will not be met. This factor will also help the courts by eliminating a hacker's intent, by assuming that if a hacker has access to these data points, the hacker is using this information for malicious purposes. Additionally, there are certain categories of PHI that HIPAA identifies as more severe than others. For example, a hacker's access to a social security number has more potential harm than merely having the patient's name. The degree of confidentiality of the breached data will also contribute to the Court's analysis of this factor in determining whether a plaintiff has standing.

B. Timeliness of the Complaint

The next relevant factor in weighing whether plaintiffs have Article III standing for potential future harms is considering when the complaint was filed. This Note adopts a point made by the Fourth Circuit in *Beck v. McDonald*, discussed above, which stated that "as the breaches fade further into the past, the Plaintiffs' threatened injuries become more and more speculative."[163] The timing of the complaint filed contributes to the *Clapper* Court's "certainly impending" standard by considering the severity of the breach by accounting for when the complaint was filed.[164] If a plaintiff waits a substantial amount of time to file suit after discovering there was a breach, a court is less likely to hold that there was a risk of "substantial harm."

The Court in *In re Zappos* considered the effect of lapsed time in a data breach suit.[165] Although not in the healthcare field, the Court's analysis regarding the timeliness of the complaint should be a relevant factor in determining whether victims of healthcare data breaches have standing. In *Zappos,* hackers targeted Zappos' servers containing the personal identifying information of approximately twenty-four million customers.[166] The following day, Zappos sent an email to its customers notifying them of the breached server and stolen data.[167] However, the

---

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

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

164. *Id.*

165. *In re* Zappos.com, 108 F. Supp. 3d 949, 958 (D. Nev. 2015).

166. *Id.* at 951.

167. *Id*.

individuals harmed did not take immediate action in filing suit.[168] The Court held that the alleged threat of future harm cannot be considered certainly impending three and a half years after the breach occurred.[169] During those three and a half years, the plaintiffs did not allege any theft or fraud.[170] The Court stated that "the more time that passes without the alleged future harm actually occurring undermines any argument that the threat of that harm is immediate, impending, or otherwise substantial."[171]

The proposition that a court should consider the passage of time is not to say that the hospital or health care facility can wait to report the breach to affected patients. Rather, this factor considers the promptness of the hospital reaching out to the patients and the turn-around of the patients filing suit upon receiving notice. If the hospital does not report the breach in a timely manner, the plaintiffs should not be penalized. In the same vein, if the hospital does notify the patients in a timely manner, the duty is on the patients to file suit quickly in order to meet the "substantial risk" standard. The HITECH Act requires that following a breach of unsecured PHI, covered entities must provide notification to affected individuals, the Secretary, and sometimes the media.[172] Covered entities must provide this individual notice in written form by first-class mail.[173] Alternatively, the covered entity may tell the patients by email if the affective individual had already agreed to receive such notices electronically.[174] These individual notifications must be provided without unreasonable delay, and in no case later than sixty-days following the discovery of a breach.[175] If a hospital meets these requirements, the duty is on the patient to promptly file suit.

The Court in *Zappos* noted that the Supreme Court in *Clapper* counseled against speculation, and the *Zappos* Court was thus apprehensive to consider the passage of time due to speculation.[176] However, this Note advocates that the passage of time is merely a consideration a court should consider and is not the definitive answer as to whether a harm is certainly impending.

C. Reasonableness of the Hospital to Maintain Security

The consideration of whether a plaintiff has Article III standing occurs early in the litigation process, that it may seem unorthodox to consider the actions of

---

168. *Id.*

169. *Id.* at 958.

170. *Id.* at 957.

171. *Id.* at 958. *See also* Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 367 (M.D. Pa. 2015) ("Indeed, putting aside the legal standard for imminence, a layperson with a common-sense notion of 'imminent' would find this lapse of time, without any identity theft, to undermine the notion that identity theft would happen in the near future.").

172. Breach Notification Rule, 45 C.F.R. §§ 164.400-414 (2009).

173. *Id.*

174. *Id.*

175. *Id.*

176. *In re* Zappos.com, 108 F. Supp. 3d 949, 958 (D. Nev. 2015).

the defendant. However, when it comes to data breaches in hospitals and the sensitivity of the PHI potentially stolen, this Note advocates that there is a public policy argument for considering the actions of the hospital.

A case that highlights the consideration of the defendants' security measures is *In re Adobe Systems.* In *Adobe,* hackers gained unauthorized access to Adobe's servers and spent several weeks inside Adobe's network without being detected.[177] The hackers gained access to sensitive data of at least thirty-eight million consumers.[178] Following the data breach, researchers concluded that Adobe's security practices were deeply flawed and did not conform to industry standard.[179] The Court found that the plaintiffs plausibly alleged that they faced a substantial, 'certainly impending' risk of harm from the data breach because "the injury is fairly traceable to Adobe's failure to abide by its contractual obligation to provide reasonable security measures."[180] Similarly, when a patient gives a hospital its PHI, there is a contractual obligation by the hospital to provide reasonable security measures.

Many hospitals contend that increasing security measures is costly and still may not protect them. The Center for Internet Security offers the Malicious Domain Blocking and Reporting ("MDBR") service at no cost to all public and private hospitals and related healthcare organizations in the United States.[181] MDBR provides an additional layer of cybersecurity protection and is a fully managed proactive domain security service.[182] MDBR proactively blocks malware, is proven effective and easy to implement, does not interfere with business operations or patient care, and comes at no cost to the healthcare institution.[183]

This factor will also act as a defense for hospitals and health care organizations who have gone above and beyond to ensure their patients' PHI is protected. Hospitals are the subject of data breaches because the healthcare system is vulnerable by design.[184] Most healthcare systems have different software packages and depend on different systems, emergency systems, X-ray software, pharmaceutical software, patient data and records management.[185] The attack surface will continue to expand as more employees work from home and

---

177. *In re* Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1206 (N.D. Cal. 2014).

178. *Id.*

179. *Id.*

180. *Id.* at 1220.

181. *No-Cost Malicious Domain Blocking and Reporting for U.S. Hospitals,* CTR. INT. SEC., https://www.cisecurity.org/hospitals [https://perma.cc/7PLD-SUGF] (last visited Feb. 1, 2022).

182. *Id.*

183. *Id.*

184. Heather Landi, *UHS Breach Shows the Dangers Facing Hospitals with Growing Ransomware Threats,* FIERCE HEALTHCARE (Oct. 2, 2020), https://www.fiercehealthcare.com/tech/uhs-breach-shows-dangers-facing-hospitals-growing-cyber-threats [https://perma.cc/G47Q-WHHB].

185. *Id.*

use network connections outside of the hospital itself.[186] Simple changes, such as two-factor authentication and utilizing unique passwords can help hospitals get ahead of data breaches.[187]

These three factors in the balancing test will better help courts discern the complicated topic of Article III standing for victims of data breaches of their PHI. It is important to note that like all balancing tests, not all factors need to point in one direction to grant or dismiss a 12(b)(6) Motion. An outstanding showing in one factor may outweigh a deficiency in another. However, in general, this Note advocates that courts should err on the side of the plaintiff to better increase their chances of being heard before a court of law. As a matter of public policy, a hospital is in the best position to ameliorate the damage done by a data breach. Bearing that the cost of litigation can be burdensome on a plaintiff, and increasing the plaintiff's chances of being heard will help urge hospitals to be proactive in cyber security.

IX. CONCLUSION

The ambiguity among the circuit courts when it comes to standing, data breaches, and healthcare is the most dangerous part of the Supreme Court's lack of clarification in *Clapper* and *Spokeo.* Although the topic of data breaches and their significant harms in the last decade is a relatively new threat to our country's healthcare sector, the Supreme Court should not shy away from making a ruling on when plaintiffs can sue their healthcare providers or hospitals.

Perhaps the apprehension for the delay in Supreme Court precedent on the topic of Article III standing for healthcare data breaches is the tension between Congress creating federal legislation and the Judiciary creating law on the topic. In light of the recent *TransUnion* opinion, this Note advocates that guidance from the judiciary would be more beneficial to society than more federal legislation. Article III standing is a "hard floor" that Congress may not circumvent,[188] which means that the question for victims is not "under what law can I bring suit?" but rather, "can I survive a motion for failure to state a claim?" Risk of future harm may seem like an abstract harm to some but is a very real anxiety and danger to victims of data breaches. Simultaneously, allowing plaintiffs to file suit for any kind of data breach could flood the courts and drive small businesses out of business.

A balancing test, although unusual for the pleading stage of litigation, seems like a solution that considers the danger to victims while also considering the unfortunate position of the defendant. Focusing the balancing test first on the healthcare sector will help the Supreme Court focus on one area of this relatively new harm instead of creating a blanket ruling. When a plaintiff has her PHI stolen, files a timely complaint, and the hospital failed to have adequate security measures in place, the plaintiff should be able to survive a 12(b)(6) Motion.

---

186. *Id.*

187. *Id.*

188. Summers v. Earth Island Inst., 555 U.S. 488, 497 (2009).

Another scenario could be that a plaintiff cannot prove that her breached data falls into one of the categories of PHI set out by HIPAA, the plaintiff did not file a timely complaint, and the hospital had security measures in place such as MDBR. The point of this balancing test is that it synthesizes the precedent set out by the Supreme Court which indicates that the "certainly impending" and "substantial risk" standard is fact specific. The balancing test proposed by this Note takes into account the multitude of ways a data breach can come about and helps weigh both the hospital and the patient's interests.