THE EFFECTS OF *CLAPPER V. AMNESTY INTERNATIONAL USA*: AN IMPROPER TIGHTENING OF THE REQUIREMENT FOR ARTICLE III STANDING IN MEDICAL DATA BREACH LITIGATION

I. INTRODUCTION

Imagine a car accident victim requiring a blood transfusion, but the medical providers used the wrong blood type because a hacker previously impersonated the victim to use his medical identity to access free health care.[1] The doctors treating the car accident victim followed the documentation on file, nonetheless, the victim sustained even more serious health problems following an incorrect transfusion.[2] After it was too late, the car accident victim found out he was also a victim of medical identity theft and suffered its most dangerous consequence—altered medical records.[3] A medical identify theft hacker may have also used the victim's health insurance to pay for hundreds of thousands of dollars' worth of surgeries, potentially making the victim's health and life insurance more expensive or unavailable.[4]

Medical identity theft occurs when a hacker—without a victim's knowledge or consent—misuses the victim's medical identity, such as records, health insurance, or personal information, to obtain medical care.[5] Medical identity theft is currently the fastest growing identity theft crime but is very difficult to detect.[6] Medical identity theft, as a type of identify theft, sometimes occurs following a data security breach.[7] However, since the United States Supreme Court decision in *Clapper v. Amnesty International USA*,[8] the majority of federal district courts around the country have dismissed data security breach victims' lawsuits, determining that a threat of future identity theft

1. Katherine M. Sullivan, *But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft*, 35 AM. J.L. & MED. 647, 651-52 (2009).

2. *Id*. at 652.

3. *Id*.

4. *Id*.; *see also* Pam Dixon, *Medical Identity Theft: The Information Crime that Can Kill You*, WORLD PRIVACY FORUM 1, 7 (2006) (discussing medical identity theft as well as outlining the great harm suffered by victims of identity theft).

5. Dixon, *supra* note 4, at 5.

6. *Id.* at 7. It is estimated "that 2.32 million adult-aged Americans or close family members became victims of medical identity theft during or before 2014. The increase from last year's estimate of 1.84 million individuals represents a net change of 21.7 percent." *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE 1, 9 (2015).

7. Dixon, *supra* note 4, at 34.

8. 133 S. Ct. 1138 (2013).

following a data breach does not constitute a sufficient injury for Article III standing.[9]

In *Clapper*, the United States Supreme Court held a group of respondents lacked standing to challenge the constitutionality of the Foreign Intelligence Surveillance Act because their claimed injury was hypothetical and not certainly impending.[10] Many federal district courts have determinedly applied the certainly impending standard to data breach lawsuits.[11] On the other hand, courts have noted that because *Clapper* did not overrule the substantial risk line of cases, plaintiffs can establish standing if there is a substantial risk that the harm will occur.[12]

This Topic Article will first discuss the facts, holding, and implications of *Clapper v. Amnesty International USA*.[13] It will then discuss several federal district court cases that, in following *Clapper*, have dismissed data breach lawsuits for a lack of standing.[14] Next, this Article will review a handful of federal court cases that have interpreted *Clapper* more narrowly to determine data breach victims successfully demonstrated an injury in fact for standing purposes.[15] This Article will then discuss a recent Supreme Court case that established standing under the substantial risk of harm standard.[16] This Article will subsequently explain the rise of medical identity theft in recent years and how its grave consequences differ from personal or financial identity theft.[17] This Article will then argue that *Clapper*'s certainly impending standard for standing should not apply to medical security breaches because *Clapper* did not even involve a data security breach, and the dangerous consequences of medical identity theft require medical security breaches to be held to a lower standing standard than financial identity theft.[18] This Article will then propose that the

9. Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *3 (E.D. La. May 4, 2015).

10. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

11. *Green*, 2015 WL 2066531, at *3; *see also* In re Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (determining plaintiffs did not suffer a certainly impending injury, therefore they lacked standing); Storm v. Paytime, Inc., 90 F. Supp.3d 359, 366 (N.D. Pa. 2015) (finding no actual injury because there was no allegation that misuse of Plaintiffs' breached confidential information was certainly impending); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 850, 854 (S.D. Tex. 2015) (finding that Peters' increased risk of future identity theft or fraud is an "attenuated chain of possibilities" rather than a certainly impending injury).

12. In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1213 (N.D. Cal. 2014).

13. *See infra* notes 22-40 and accompanying text.

14. *See infra* notes 41-58 and accompanying text.

15. *See infra* notes 59-81 and accompanying text.

16. *See infra* notes 82-91 and accompanying text.

17. *See infra* notes 93-122 and accompanying text.

18. *See infra* notes 123-168 and accompanying text.

substantial risk of harm standard should instead apply to medical security breach claims in order to allow victims to have the merits of their cases heard.[19] It will discuss the potential objections to this Article's alternative proposal and offer a response to those objections.[20]

II. BACKGROUND

A. *Clapper v. Amnesty International USA*: Effects on Data Security Breach Claims

In *Clapper v. Amnesty International USA*,[21] the respondents brought a claim involving a constitutional challenge to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), codified at 50 U.S.C. § 1881a.[22] To gather foreign intelligence information, FISA authorizes the Attorney General and Director of National Intelligence to gather surveillance information on non-United States persons who are reasonably believed to be outside the United States.[23] The respondents challenging FISA were attorneys and labor, human rights, media, and legal organizations that electronically communicated with clients outside the United States and believed their clients were likely targets of the FISA surveillance.[24] The respondents sought a declaration that section 1881a was unconstitutional and an injunction to prohibit surveillance authorized by section 1881a.[25] They argued that section 1881a inhibited their ability to find witnesses and sources, gather information, and confidentially communicate with their clients.[26]

The issue on appeal was whether the respondents had standing to challenge FISA.[27] The respondents argued two sources of injuries for standing purposes.[28] First, there was an objectively reasonable likeli-

19. *See infra* notes 169-184 and accompanying text.
20. *See infra* notes 185-201 and accompanying text.
21. 133 S. Ct. 1138 (2013).
22. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144 (2013).
23. *Clapper*, 133 S. Ct. at 1142. The intention of FISA, as enacted in 1978, was to allow government surveillance of certain communications for foreign intelligence reasons. *Id.* Surveillance was authorized if there was probable cause to believe the targets were agents of a foreign power. *Id*. The 2008 amendment to FISA included section 1881a, which did not require the government to show probable cause in order to perform electronic surveillance on non-United States persons (United States persons are defined as "citizens of the United States, aliens for permanent residence, and certain associations and corporations") linked to a foreign power. *Id.* at 1143-44.
24. *Id.* at 1145.
25. *Id*. at 1142.
26. *Id*. at 1145.
27. *Id*. at 1142. To establish standing, a plaintiff must establish it has an actual or imminent injury in fact that is concrete and particularized, the injury is fairly traceable to the defendant's challenged action, and a favorable judicial decision will likely redress the injury. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).
28. *Clapper*, 133 S. Ct. at 1146.

hood that section 1881a would allow gathering of their international communications in the future, and second, section 1881a compelled them to protect their foreign communications through costly and burdensome measures because there was a substantial risk their communication would be subject to section 1881a surveillance.[29] The United States District Court for the Southern District of New York determined that respondents failed to establish standing in order to challenge section 1881a.[30] On appeal, the United States Court of Appeals for the Second Circuit reversed, reasoning the plaintiffs satisfied the injury-in-fact requirement of standing because it was reasonably likely that their international communications would be monitored under section 1881a.[31] The United States Supreme Court granted certiorari because the constitutionality of section 1881a was an important issue and the Court of Appeals adopted an unusual view of standing.[32]

The Supreme Court emphasized how a threatened injury must be certainly impending to satisfy the injury-in-fact requirement of standing and alleging a possible future injury is insufficient.[33] The Court rejected the Second Circuit's objectively reasonable likelihood standard of establishing a certainly impending injury-in-fact.[34] The Court ultimately held respondents lacked standing because their claimed injury, based on a hypothetical harm and an attenuated sequence of possibilities, was not certainly impending.[35] The Court also noted that even if respondents did establish an injury-in-fact, they would fail to demonstrate that their injury was fairly traceable to section 1881a because they could only speculate that section 1881a authorized surveillance of their international communications.[36]

While *Clapper* was a constitutional challenge of FISA and factually unrelated to a typical data breach claim, *Clapper* has had larger effects across the country in the last two years with data breach plain-

29. *Id*.

30. Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009).

31. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 139 (2d Cir. 2011). The Second Circuit stated that the plaintiffs' fears of future surveillance were not speculative. *Clapper*, 638 F.3d at 139.

32. *Clapper*, 133 S. Ct. at 1146.

33. *Id*. at 1147 (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)); *see also* Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979) (stating that a certainly impending threat of injury is enough to establish standing); City of L.A. v. Lyons, 461 U.S. 95, 101 (1983) (asserting that a plaintiff must show his threat of injury is real and immediate, not hypothetical or conjectural, to satisfy the injury-in-fact requirement of standing).

34. *Clapper*, 133 S. Ct. at 1147.

35. *Id*. at 1143. Whether the Government would have imminently targeted respondents' communications was only speculative. *Id*. at 1148.

36. *Id*. at 1148. Thus, they would fail the second prong of Article III standing. *Id*.

tiffs having difficulty establishing standing in data security class action claims.[37] In the last two years, many federal courts across the United States have dismissed data breach claims because plaintiffs have struggled to establish that their increased risk of future harm is certainly impending.[38] However, federal courts have not settled what constitutes a sufficient injury for standing in data breach cases.[39]

B. District Court Cases Dismissed For Lack of Standing Post-*Clapper*

Since the United States Supreme Court's decision in *Clapper v. Amnesty International USA*,[40] was announced in February 2013, there have been at least eight data security breach cases dismissed for lack of standing in federal district courts.[41] In *Green v. eBay Inc.*,[42]

37. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 656 (S.D. Ohio 2014) (reasoning that an increased risk of identity theft may have previously satisfied the "objectively reasonable likelihood" or "not merely speculative" standards for standing, "but under *Clapper*, more is required to show an injury is certainly impending.").

38. *See*, *e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 854, 857 (S.D. Tex. 2015) (granting the defendant's motion to dismiss because an increased risk of future identity theft does not satisfy the certainly impending standard); In re Sci. Applications Int'l Corp. ("SAIC") Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25, 28 (D.D.C. 2014) (reasoning a risk of future identity theft is speculative and fails to meet the injury-in-fact standing requirement); Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (determining that plaintiffs' claim of a future identity theft is too hypothetical to satisfy the certainly impending standard discussed in *Clapper*).

39. *See, e.g.*, Bliss & Glennon Inc. v. Ashley, 420 S.W.3d 379, 390 (Tex. App. 2014) (noting that "the question of what a plaintiff must allege to establish standing in data-breach cases is far from settled under federal law.").

40. 133 S. Ct. 1138 (2013).

41. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 854, 857 (S.D. Tex. 2015) (granting the defendant's motion to dismiss because an increased risk of future identity theft does not satisfy the certainly impending standard); Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (determining that plaintiffs' claim of a future identity theft is too hypothetical to satisfy the certainly impending standard discussed in *Clapper*); In re Horizon Healthcare Servs., Inc. Data Breach Litig., 2015 WL 1472483, at *6 (D.N.J. March 31, 2015), *appeal docketed*, No. 15-2309 (3d Cir. June 1, 2015) (determining plaintiffs do not have standing because an increased risk of future harm is insufficient and they did not allege a post-breach misuse of their compromised data); Storm v. Paytime, Inc., 90 F.Supp.3d 359, 366 (M.D. Pa. 2015) (finding no actual injury because there was no allegation that misuse of Plaintiffs' breached confidential information was certainly impending); Lewert v. P.F. Chang's China Bistro, Inc., 2014 WL 7005097, at *3-4 (N.D. Ill. Dec. 10, 2014), *appeal docketed*, No. 14-3700 (7th Cir. Dec. 12, 2014) (maintaining that an increased risk of identity theft does not constitute an injury-in-fact, and dismissing the claim for a lack of standing); *In re SAIC*, 45 F. Supp. 3d at 25, 28 (reasoning a risk of future identity theft is speculative and fails to meet the injury-in-fact standing requirement); *Galaria*, 998 F. Supp. 2d at 657 (holding that plaintiffs' increased risk of identity theft, medical fraud, identity fraud, or phishing is not sufficient to meet the certainly impending injury-in-fact threshold to constitute standing); Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 456, 471 (D.N.J. 2013) (dismissing plaintiffs' claim for a lack of standing after Omnicell's laptop containing plain-

the United States District Court for the Eastern District of Louisiana found that the plaintiff failed to establish a certainly impending injury-in-fact.[43] Unknown hackers accessed eBay's files that contained personal information of its users, including names, passwords, birth dates, email addresses, home addresses, and phone numbers.[44] A consumer privacy putative class action was filed against eBay, and eBay filed a motion to dismiss the complaint for lack of standing, arguing no one had attempted to commit identity fraud with the eBay users' information.[45] eBay then contended the United States Supreme Court's decision in *Clapper* made it clear that a speculative possibility of a future injury does not constitute an injury-in-fact for standing purposes.[46] The district court cited numerous other district courts that have dismissed data breach claims for lack of standing since the *Clapper* decision.[47] Aligning with these other decisions, the court stated the plaintiff had not alleged a certainly impending threat of future identity fraud or theft because the plaintiff did not satisfy numerous variables the court deemed relevant to establish injury-in-fact.[48] The district court dismissed the plaintiff's complaint without prejudice for lack of standing.[49]

Similarly, in *Peters v. St. Joseph Services Corp.*,[50] the United States District Court for the Southern District of Texas found that Peters, as the representative of a class action lawsuit, did not have standing because an increased risk of future identity theft after a data security breach does not constitute a cognizable injury.[51] Hackers breached the computer network of St. Joseph's, a health care provider

---

tiffs' medical information was stolen in a data breach); In re Barnes & Noble Pin Pad Litig., 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (stating that an increased risk of identity theft does not establish standing because the increased risk of harm is not certainly impending).

42. No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015).

43. Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *4 (E.D. La. May 4, 2015).

44. *Green*, 2015 WL 2066531, at *1. eBay also collects its users' credit card and bank account information, but "there is no indication that any financial information was accessed or stolen during the Data Breach." *Id*.

45. *Id*. at *1-2.

46. *Id*.

47. *Id*. at *3.

48. *Id*. at *5. The district court noted how "an increase in the risk of harm is irrelevant—the true question is whether the harm is certainly impending." *Id*. The variables affecting whether the plaintiffs became identity theft victims included "whether their data was actually taken when it was accessed, whether certain information was decrypted, whether the date was actually misused or transferred to another third party and misused, and whether or not the third party succeeded in misusing the information." *Id*.

49. *Id*. at *6.

50. 74 F. Supp. 3d 847 (S.D. Tex. 2015).

51. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 849-50 (S.D. Tex. 2015).

in Texas, which subjected more than 400,000 individuals to a data security breach.[52] Peters argued the class members were more likely to be victims of identity theft crimes in the future, and St. Joseph, citing *Clapper*, moved to dismiss the complaint for lack of standing.[53] The district court stated Peters' possible future injury of identity theft was speculative and not certainly impending.[54]

Additionally, in the case *In re Horizon Healthcare Services, Inc. Data Breach Litigation*,[55] the class action plaintiffs sued Horizon Healthcare Services, Inc., a health insurance company, after an unknown thief stole laptops from Horizon's headquarters.[56] The laptops held more than 839,000 individuals' personal and medical information.[57] The plaintiffs alleged an imminent and continuing increased risk of identity fraud, identity theft, and medical fraud, but the district court reasoned that plaintiffs lacked standing because their risk of future injury was hypothetical and attenuated.[58]

C. Federal Court Cases Where Data Breach Victims Have Established Standing

Conversely, district courts in the Ninth Circuit have not concluded that *Clapper* has made it more difficult for plaintiffs to establish an injury-in-fact for standing purposes.[59] For example, in the case *In re Sony Gaming Networks and Customer Data Security Breach Litigation*,[60] the plaintiffs brought a class action lawsuit against Sony Computer Entertainment America, LLC, Sony Network Entertainment America, Inc., and Sony Online Entertainment, LLC, (collectively, "Sony"), after their personal information stored on Sony's network via individual gaming consoles was compromised by criminal hackers.[61] Sony filed a motion to dismiss, arguing the plaintiffs lacked standing after the *Clapper* decision.[62] The United States District Court for the Southern District of California disagreed, and it discussed how the decision in *Clapper* did not change standing re-

52. *Peters*, 74 F. Supp. 3d at 850.
53. *Id*. at 851.
54. *Id*. at 854. The district court dismissed Peters' federal claims with prejudice. *Id*. at 857.
55. No. 13-7418, 2015 WL 1472483 (D.N.J. March 31, 2015).
56. In re Horizon Healthcare Serv., Inc. Data Breach Litig. (*Horizon Healthcare*), No. 13-7418, 2015 WL 1472482, at *1 (D.N.J. March 31, 2015), *appeal docketed*, No. 15-2309 (3d Cir. June 1, 2015).
57. *Horizon Healthcare*, 2015 WL 1472482, at *1.
58. *Id.* at *1, *6.
59. In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (*Sony Gaming*), 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014).
60. 996 F. Supp. 2d 942 (S.D. Cal. 2014).
61. *Sony Gaming*, 996 F. Supp. 2d at 954-55.
62. *Id*. at 960.

quirements, nor did it overrule Court of Appeals for the Ninth Circuit precedent.[63] Therefore, relying on the Ninth Circuit precedent, the United States District Court for the Southern District of California denied Sony's motion to dismiss because Sony collected and wrongfully disclosed plaintiffs' personal information, which created a sufficiently credible threat of impending harm to establish standing.[64]

In *Remijas v. Neiman Marcus Group, LLC*,[65] the United States Court of Appeals for the Seventh Circuit reversed the United States District Court for the Northern District of Illinois' dismissal, determining that the data breach victims sufficiently met the standing requirements.[66] The victims, customers of Neiman Marcus department stores whose credit card numbers were stolen by hackers, brought a class action lawsuit against Neiman Marcus.[67] The Seventh Circuit stated that the district court incorrectly understood *Clapper* to bar any future injuries as sufficient for standing.[68] Demanding that data breach victims must wait until the potential harm materializes into identify theft would make it more difficult for plaintiffs to successfully argue their injury-in-fact was fairly traceable to the data breach.[69] Therefore, the Seventh Circuit determined the data breach victims presented enough evidence to demonstrate a substantial risk of harm, thereby establishing an injury-in-fact.[70] Because the plaintiffs met

---

63. *Id*. at 961. The court in *Sony Gaming* explained that in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the plaintiffs established standing based on a "credible threat of harm" that was not hypothetical. *Sony Gaming*, 996 F. Supp. 2d at 961. "Therefore, although the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be 'certainly impending,' rather than 'real and immediate . . . ,'" the Supreme Court did not overrule the Ninth Circuit's standing precedent. *Id*.

64. *Id*. at 961-62; *see also* In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1213-14 (N.D. Cal. 2014) (stating that *Clapper* did not alter the standing framework and noting how *Clapper* addressed whether a political branch of government violated the Constitution).

65. 794 F.3d 688 (7th Cir. 2015).

66. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).

67. *Remijas*, 794 F.3d at 690. Thousands of victims alleged they incurred fraudulent charges on their credit cards, but the main issue on appeal involved victims who alleged a concrete risk of harm and possible future identity theft. *Id*. at 692.

68. *Id*. at 693. The Seventh Circuit discussed that the Supreme Court in *Clapper* "did not jettison the 'substantial risk standard.'" *Id*. "To the contrary, [*Clapper*] stated that '[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about.'" *Id*. (citing *Clapper*, 133 S. Ct. at 1150 n.5).

69. *Id*. This addresses the second prong of standing as established by the Supreme Court's decision in *Lujan*. *Id*. at 691-92; *see also* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (determining that an injury-in-fact must be fairly traceable to the defendant's challenged conduct).

70. *Id*. at 693, 696. "Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id*. at 693. The court articulated that while the plaintiffs must provide a factual basis for their increased risk

the standing requirements, the Seventh Circuit reversed the lower court's decision to grant Neiman Marcus's motion to dismiss and remanded the case for further proceedings.[71]

Additionally, in *Moyer v. Michaels Stores, Inc.*,[72] the defendant argued *Clapper* tightened the standing requirements for injuries based on a future risk of harm, but the United States District Court for the Northern District of Illinois disagreed.[73] The *Moyer* court noted the certainly impending standard to satisfy the injury-in-fact requirement of standing was applied rigorously in *Clapper* because the Supreme Court addressed the constitutionality of a congressional law in light of a national security issue.[74] The district court stated that connecting a data security breach to identity theft in the future is not an attenuated chain of possibilities so as to make the possible identity theft speculative or hypothetical.[75] Thus, the court concluded the increased risk of identity theft after a data security breach satisfied the imminence requirement to establish standing.[76]

In the case, *In re Target Corporation Data Security Breach Litigation*,[77] the United States District Court for the District of Minnesota found the data victims sufficiently alleged an injury for standing purposes.[78] The data breach resulted in roughly 110 million Target customers having their financial information compromised.[79] Target filed a motion to dismiss, arguing the plaintiffs did not have an actual or imminent injury to meet the standing requirement.[80] Without ever citing *Clapper*, the court concluded the class action plaintiffs had standing to survive the motion to dismiss.[81]

---

of future identify theft down the road in litigation, "[t]heir allegations of future injury are sufficient to survive a 12(b)(1) motion." *Id*. at 694.

71. *Id*. at 697.

72. No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).

73. Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *4-5 (N.D. Ill. July 14, 2014); *but see* Strautins v. Trustware Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) (stating that *Clapper* requires the Court to find "that an increased risk of identity theft" fails to satisfy the injury-in-fact requirement for standing); In re Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588, at *3 (N.D. Ill. Sept. 3, 2013) (refusing to accept plaintiffs' "increased risk of identity theft" claim as sufficient to establish standing).

74. *Moyer*, 2014 WL 3511500, at *6.

75. *Id*.

76. *Id*.

77. 66 F. Supp. 3d 1154 (D. Minn. 2014).

78. In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

79. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1157.

80. *Id*. at 1158-59.

81. *Id*. at 1159.

D. *Monsanto Company v. Geertson Seed Farms*: Standing Established Under the Substantial Risk of Harm Standard

In *Monsanto Co. v. Geertson Seed Farms*,[82] the United States Supreme Court concluded the respondents had standing to challenge the deregulation of Roundup Ready Alfalfa ("RRA"), a type of genetically engineered alfalfa crop that can tolerate the herbicide Roundup.[83] Respondents included environmental groups focused on food safety and two farms utilizing conventional alfalfa seeds.[84] Based on its finding that RRA would likely have no significant environmental impact, the Animal and Plant Health Inspection Service ("APHIS"), a division of the Department of Agriculture, granted non-regulated status to RRA and authorized RRA field trials.[85] The respondents challenged APHIS's deregulation of RRA, arguing that as conventional alfalfa farmers, the engineered gene in RRA would harm conventional alfalfa crops if RRA were deregulated completely.[86]

The Supreme Court determined there was a substantial risk the gene flow from the RRA to respondents' traditional alfalfa crops would injure respondents in numerous ways.[87] Specifically, if these traditional alfalfa farmers wanted to continue promoting their alfalfa product as non-genetically-engineered, they would need to test their crops for genetically engineered alfalfa contamination.[88] Additionally, the risk of gene flow to traditional alfalfa crops would require the respondents to curtail potential contamination through preventative measures.[89] Because there was a substantial risk that these harms would occur, the Court stated that the harms were concrete enough to meet the injury-in-fact requirement for standing.[90] Therefore, the Court reasoned that the substantial risk of these potential harms established an injury-in-fact even if the respondents' traditional crops were never actually infected; thus, the traditional alfalfa farmers demonstrated standing.[91]

---

82. 561 U.S. 139 (2010).

83. Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 146, 156 (2010). "Monsanto owns the intellectual property rights to RRA." *Monsanto*, 561 U.S. at 146.

84. *Id*.

85. *Id*. at 145-46.

86. *Id*. at 153.

87. *Id*. at 153-54. In its application of the substantial risk standard to respondents' injury, the Court noted how the United States District Court for the Northern District of California had found that the traditional alfalfa farmers "established a 'reasonable probability' that their organic and conventional alfalfa crops will be infected" because of "the undisputed concentration of alfalfa seed farms . . . ." *Id.* at 153.

88. *Id*. at 154.

89. *Id*.

90. *Id.* at 155.

91. *Id*. at 153, 155.

E. The Rise of Medical Identity Theft in Recent Years

A data breach means there is a loss, theft, or unauthorized access to someone's confidential personal information contained in electronic data.[92] Identity theft subsequently occurs when someone's personal information is misused or used without permission for fraudulent purposes.[93] State law regulates most data breach notification laws and there is variation as to what each state requires.[94] Accordingly, it is difficult for large businesses that engage in interstate commerce to comply with the different laws of each state.[95] On the other hand, there is no single law that regulates the security of private personal information at the federal level.[96] Instead, federal regulation of data security is sector specific.[97]

Medical identity theft, as a subcategory of identity theft, involves theft or unauthorized use of another person's personal information to acquire or bill for medical goods or services.[98] Medical identity theft usually arises in two forms: using a person's identification without their knowledge or consent, such as a Social Security Number, to receive medical care or purchase medical goods, or using a person's identity to pay for medical services or goods.[99] Medical identity theft is dangerous because while forging a claim to pay for medical services, a hacker often falsifies the victim's medical records to support his fraudulent claim.[100] These changes can occur on purpose or unintentionally, and often victims and healthcare providers do not realize the falsification immediately, if ever.[101] While medical identity theft has potentially devastating effects, it is not studied or documented as well as other forms of identity theft and is the most problematic identity

92. Gina Stevens, Cong. Research Serv., R42475, Data Security Breach Notification Laws 1 (2012).

93. Stanley C. Ball, *Ohio's "Aggressive" Attack of Medical Identity Theft*, 24 J.L. & Health 111, 115 (2010).

94. Stevens, *supra* note 92, at 3-4.

95. *Id*. at 5.

96. *Id*. at 7.

97. *Id*. Federal law imposes data protection obligations on certain sectors, such as "credit, financial services, healthcare, government, securities, and Internet sectors." *Id*.

98. Dep't of Health & Hum. Servs., *CMS Response to Breaches and Medical Identity Theft*, Dep't of Health & Hum. Servs., 1 (2012), *available at* http://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf.

99. Laurie A. Rinehart-Thompson, *Raising Awareness of Medical Identity Theft*, J. Am. Health Info. Mgmt. Ass'n 79, 74, no. 10 (Oct. 2008).

100. *Id.* at 74. The perpetrator may enter his or her own physical or mental traits into the victim's health records, which can "expose[ ] the victim to improper and potentially life-threatening treatment if critical medical conditions, procedures, medications, and allergies are either omitted from the record or wrongfully included." *Id*.

101. Dixon, *supra* note 4, at 6. Medical identity theft victims can receive incorrect medical treatment, have their health or life insurance policies denied or spent, fail an employer's physical exam because of false diagnoses, or have their medical histories altered. *Id*.

theft crime to correct because there are limited remedies and rights available to victims.[102]

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH Act")[103] to alter regulations of the private health information system.[104] Under the HITECH Act, the Department of Health and Human Services and Federal Trade Commission were required to create notification requirements, so victims of data breaches would be alerted of an alteration or potential alteration to their medical records.[105] However, the data protection model set up by HIPAA and the updates provided by HITECH to protect patients from data breaches are still flawed.[106] Unlike financial identity theft victims, medical identity theft victims have few private remedies available.[107] This is problematic because medical identities are extraordinarily valuable to criminals.[108] Medical identity theft is also easier to commit because health care systems have switched to electronic medical records, disseminating medical errors through many healthcare providers.[109] A recent medical identity theft survey estimated that in 2014 there were 481,657 additional medical identity theft cases than in the previous year.[110] While the complex HIPAA scheme touches on numerous issues faced by the health care industry, HIPAA does not actually provide a private right of action.[111] Thus, victims of medical identity theft can only bring claims under a state cause of action.[112] Alternatively, these victims have no other choice but to watch from the sidelines as the Secretary

---

102. *Id*. at 5.

103. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, § 3000, 123 Stat 115 (2009) (codified at 42 U.S.C. §§ 300jj through 300jj–51).

104. Stevens, *supra* note 92, at 13. Among other things, HITECH brought more businesses under the HIPAA Privacy and Security Rules, included civil and criminal liability provisions, gave state attorneys general authority to bring claims in federal district court to enforce HIPAA violations, added data breach notification requirements. *Id*.

105. Sullivan, *supra* note 1, at 662-63.

106. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX: JOURNAL OF LAW-MEDICINE 65, 68 (2014). "HIPAA does not literally protect data." *Id*. at 69.

107. Sullivan, *supra* note 1, at 649; *see also* Dixon, *supra* note 4, at 8-9 (discussing that medical identity theft victims do not have the same rights to correct errors in their medical files as victims of financial identity theft have to correct their credit reports).

108. Terry, *supra* note 106, at 72.

109. Dixon, *supra* note 4, at 5.

110. *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE 1, 9 (2015). The rise of medical identity theft is unsurprising because healthcare providers are the largest collectors of personal data. Sullivan, *supra* note 1, at 648.

111. Sullivan, *supra* note 1, at 662, 666.

112. *Id*. at 666.

of Health and Human Services reprimands the breaching party, without alleviating the injury suffered by the breach victims.[113]

As an example of state law adjudication, the Supreme Court of Appeals of West Virginia determined the plaintiffs who claimed a medical data breach established standing because they had a legal interest in maintaining confidential medical information.[114] The plaintiffs were patients whose confidential information stored in the Charleston Area Medical Center database was accidentally placed on the Internet.[115] The respondents stated that plaintiffs' breached medical information could be discovered if someone conducted an advanced Internet search.[116] The Circuit Court of Kanawha County asserted the plaintiffs lacked standing because their claim of hypothetical future identity theft was not a concrete and particularized injury.[117] The plaintiffs appealed to the Supreme Court of Appeals of West Virginia, which agreed with the circuit court that an increased risk of future identity theft does not satisfy the injury-in-fact requirement for standing.[118] However, the highest West Virginia court reversed the circuit court because the plaintiffs, as patients of Charleston Area Medical Center, satisfied standing through their breach of confidentiality and invasion of privacy state claims.[119]

Nevertheless, invasion of privacy and breach of confidentiality do not fully encompass medical identity theft.[120] While plaintiffs in data breaches can sometimes bring a claim under state law, the implications of placing private medical records in the public domain through litigation causes many plaintiffs to forego bringing a claim at all.[121] With medical identity theft on the rise as the fastest growing crime in America, a lack of full recovery under state law, gaps in federal laws, and the recent trend in federal courts post-*Clapper* to dismiss data breach victims' lawsuits for lack of standing, data breach victims are not fully compensated for their injuries.[122]

---

113. Polanco v. Omnicell Inc., 988 F. Supp. 2d 451, 469 (D.N.J. 2013).

114. Tabata v. Charleston Area Med. Center, Inc., 759 S.E.2d 459, 464 (W.Va. 2014); *but see* Maglio v. Advocate Health & Hosps. Corp., 2015 Ill. App. 2d 140782, at *7 (2015) (finding *Tabata* distinguishable because here, plaintiffs' data, taken from their hospital records, has not been publicly disclosed nor did it lead to identity fraud for "nearly two years since the burglary[,]" while the data in *Tabata* was published on the Internet).

115. *Tabata*, 759 S.E.2d at 462.

116. *Id*.

117. *Id*. at 463-64. During discovery, the parties did not find "any unauthorized and malicious users attempting to access" the plaintiffs' confidential information, so the plaintiffs suffered no actual or attempted identity theft or other economic losses. *Id.*

118. *Id*. at 464.

119. *Id*.

120. Sullivan, *supra* note 1, at 667.

121. *Id*. at 666.

122. *Id*. at 677-78; *see also* Johnathan Rhodes, *Protecting Personal Information from Identity Theft: An Integrated Approach*, 80 J. KAN. B.A. 18, 20 (2011) (stating "medical

III. ARGUMENT

Since *Clapper v. Amnesty International USA*,[123] most federal district courts have determined that a threat of future identity theft following a data breach does not constitute a sufficient injury to establish standing.[124] At a minimum, an alleged future injury must be certainly impending in order to satisfy the standing requirements.[125] *Clapper's* indirect tightening of the injury-in-fact requirement should not apply to a threat of future medical identity theft following a data breach of a healthcare provider's stored information for two reasons.[126] First, the facts of *Clapper* did not involve a data security breach.[127] Second, even if *Clapper* correctly elevated standing as a more difficult hurdle to overcome in data security litigation, medical information compromised in a security breach must be held to a different standard than financial information compromised in a security breach.[128] Security breach plaintiffs have struggled to successfully proceed to the merits of their cases post-*Clapper*, as most claims have been dismissed at the motion to dismiss stage for failing to establish a certainly impending injury-in-fact.[129] Under the current scheme, medical data breach victims have two general options to redress their injuries: (1) they can bring a cause of action under state law if a particular state provides the remedy, such as breach of confidentiality, or (2) wait as the Secretary of Health and Human Services

---

identity theft has been labeled as the nation's fastest growing crime."); In re Zappos .com, Inc., No. 3:12-cv-00325-RCJ-VPC, 2015 WL 3466943, at *4 (D. Nev. June 1, 2015) (noting how since *Clapper* was decided, "[t]he majority of courts" have dismissed data breach cases for lack of standing).

123. 133 S. Ct. 1138 (2013).

124. *See, e.g.*, Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5 (E.D. La. May 4, 2015) (determining that plaintiffs' claim of a future identity theft is too hypothetical to satisfy the certainly impending standard discussed in *Clapper*); Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015) (finding no actual injury because there was no allegation that misuse of Plaintiffs' breached confidential information was certainly impending); Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 854 (S.D. Tex. 2015) (noting that Peters' increased risk of future identity theft or fraud is an "attenuated chain of possibilities" rather than a certainly impending injury).

125. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

126. *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014) (discussing how *Clapper*'s analysis of a certainly impending injury was "especially rigorous" in light of constitutional and national security issues); Dixon, *supra* note 4, at 17 (explaining how victims of medical identity theft do not always detect the changes but can suffer from serious medical complications if the discrepancies in their medical records are not noticed before a medical emergency).

127. *See Clapper*, 133 S. Ct. at 1145 (discussing how respondents challenged the constitutionality of the Foreign Intelligence Surveillance Act).

128. *See* Sullivan, *supra* note 1, at 649 (noting the differences between financial and medical identity theft remedies).

129. *See In re Zappos.com*, 2015 WL 3466943, at *4 (stating that "[t]he majority of courts dealing with data-breach cases post-*Clapper* have held . . . the increased risk of [identity theft] alone is insufficient" to establish standing).

reprimands a medical security breacher but often does not remedy the harm the victim personally suffered.[130] State tort law often does not fully encompass medical identity theft, so plaintiffs who bring their security breach claims in state court are not fully compensated for their injury.[131] This is especially problematic in light of federal courts' tendencies since the *Clapper* decision in 2013 to dismiss data breach cases at the motion to dismiss stage.[132]

A. *Clapper* Did Not Involve a Data Security Breach so its Application is Inappropriate

Lower federal courts' assumption that standing is more difficult to establish is tenuous because *Clapper v. Amnesty International USA*[133] did not involve a data security breach.[134] The United States Supreme Court in *Clapper* noted that the purpose of standing is to prevent the judicial branch from infringing upon the Executive and Legislative branches' powers.[135] In light of the purpose of standing, the Court's standing examination is particularly rigorous when questioning whether an Executive or Legislative branch's action is constitutional.[136] Additionally, the Court has repeatedly determined plaintiffs lack standing to challenge a political branch's foreign affairs and intelligence gathering actions.[137] Therefore, *Clapper* correctly de-

130. Sullivan, *supra* note 1, at 666; *see also* Polanco v. Omnicell Inc., 988 F. Supp. 2d 451, 469 (D.N.J. 2013) (providing that the Secretary of Health and Human Services has the ability to enforce and remedy HIPAA violations).

131. Sullivan, *supra* note 1, at 670.

132. *See Green*, 2015 WL 2066531, at *6 (ordering the data breach plaintiffs' complaint to be dismissed for lacking standing).

133. 133 S. Ct. 1138 (2013).

134. *Compare* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *6 (N.D. Ill. July 14, 2014) (discussing whether *Clapper*'s rigorous application of the certainly impending standard to its standing analysis should apply in cases that do not address national security or constitutional issues is undecided), *with* Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 n.11 (N.D. Ill. 2014) (noting how reasonable minds can differ on *Clapper's* significance in a standing analysis and answering whether a risk of identity theft establishes standing).

135. *See Clapper*, 133 S. Ct. at 1146 (explaining that "standing, which is built on separation-of-powers principles, serves to prevent the judicial process from being used to usurp the powers of the political branches."); *see also* Allen v. Wright, 468 U.S. 737, 752 (1984) (maintaining that the law of standing is grounded in the principle of separation of powers).

136. *Id*. at 1147 (quoting Raines v. Byrd, 521 U.S. 811, 819-20 (1997)).

137. *See e.g.*, United States v. Richardson, 418 U.S. 166, 168-70 (1974) (concluding that the plaintiff lacked standing to challenge the constitutionality of a legislative act allowing the Central Intelligence Agency to account for its expenditures); Schlesinger v. Reservists Committee to Stop the War, 418 U.S. 208, 209-10 (1974) (holding that plaintiffs lacked standing to challenge the constitutionality of Congressional membership in the Reserves); Laird v. Tatum, 408 U.S. 1, 10, 13 (1972) (explaining that plaintiffs failed to establish an injury for standing when challenging the Army's intelligence-gathering program, which falls under the Executive branch).

termined the respondents lacked standing to challenge the Foreign Intelligence Surveillance Act because their claimed injury was too speculative.[138]

Since *Clapper*, lower federal courts have repeatedly found that data security breach plaintiffs lacked standing because a heightened risk of future harm, such as identity theft or fraud, does not satisfy the certainly impending injury-in-fact requirement extensively discussed by the *Clapper* court.[139] Most of these district court decisions stated that *Clapper* tightened the standing requirements.[140] Admittedly, *Clapper* did emphasize how the Court has repeatedly asserted that allegations of *possible* future injury are not sufficient to meet the certainly impending standard.[141] Further, the Court repeated its reluctance to allow standing based on speculation of whether an independent actor would take action in the future.[142]

Filing a claim for a data security breach injury is not equivalent to *Clapper*'s constitutional challenge of a foreign intelligence surveillance law.[143] Partly due to the decision in *Clapper*, what satisfies the injury-in-fact requirement of standing in data security breach claims is unsettled.[144] In *Clapper,* the United States Supreme Court did not overrule any precedent, nor did it change the requirements of stand-

138. *Compare Clapper*, 133 S. Ct. at 1148 (noting that an "attenuated chain of possibilities does not" meet standing requirements of a certainly impending injury, especially in the foreign intelligence and national security realm), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (discussing how *Clapper* does not completely rule out using a future injury to support standing for data breach victims).

139. *See, e.g., Green*, 2015 WL 2066531, at *5 (determining plaintiffs' potential injury was hypothetical and did not show the risk of future identity theft was certainly impending); *Storm*, 90 F. Supp. 3d at 366 (finding a financial data breach does not constitute a certainly impending misuse); *Peters*, 74 F. Supp. 3d at 854 (noting an increased risk of future identity theft does not satisfy the certainly impending standard).

140. *See Strautins*, 27 F. Supp. 3d at 876 (noting how *Clapper* discussed the elasticity of the imminence requirement, but *Clapper* still requires the court to find an increased risk of identity theft as insufficient for standing); *but see* In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1213 (N.D. Cal. 2014) (explaining that the Supreme Court's decision in *Clapper* did not overrule any standing precedent, nor did it alter the injury-in-fact, causation, and redressability requirements of standing).

141. *Clapper*, 133 S. Ct. at 1147; *see also* Whitmore v. Arkansas, 495 U.S. 149, 156-58 (1990) (finding that petitioner did not have standing to challenge another inmate's validity of death penalty sentence because his claimed injury was too speculative).

142. *Id*. at 1150.

143. *Compare Remijas*, 794 F.3d at 694 (stating that "it is important not to overread *Clapper*"), *with In re Adobe*, 66 F. Supp. 3d at 1214 (noting that *Clapper*'s analysis of standing centered around whether a political branch of the Government violated the Constitution, which is a sensitive topic, making its analysis unusually rigorous).

144. *See* In re Zappos.com, Inc., No. 3:12-cv-00325-RCJ-VPC, 2015 WL 3466943, at *4-5 (D. Nev. June 1, 2015) (discussing that many courts have concluded an increased risk of identity theft alone does not satisfy the injury-in-fact requirement for standing, while other courts "have held the opposite").

ing.[145] Even if *Clapper* had overruled *Krottner v. Starbucks Corp.*,[146] a heightened risk of future harm when someone's personal information has been violated in a data security breach still satisfies the injury-in-fact requirement of standing.[147]

Further, *Clapper* involved an attenuated chain of causation regarding the respondents' potential future injury if the government collected sensitive information while monitoring communications between respondents and their clients outside the United States.[148] One reason district courts have made the assumption that *Clapper* has generated more strict standing requirements is because *Clapper* discussed how an injury is hypothetical if the injury's existence depends on a third party's decision.[149] Thus, courts have assumed *Clapper's* third party decision-making principle applies to data breach plaintiffs because most data breach victims' injuries depend on whether a third party, the data hacker, decides to do anything with the confidential information.[150] In contrast, a data security breach and the ensuing future injury, identity theft, are not as attenuated as *Clapper*'s facts involving potential surveillance of foreign communications.[151] Unlike *Clapper*, where it was speculative whether or not respondents' international communications would be monitored, hackers have deliberately stolen data breach plaintiffs' personal information with the intention of misusing that data.[152] Furthermore, the Ponemon Institute's 2012 survey found that more than half of all

145. *In re Adobe*, 66 F. Supp. 3d at 1213-14; *see also* In re Sony Gaming Networks & Customer Data Sec. Breach Litig. 996 F. Supp. 2d 942, 961 (S.D. Cal. 2014) (explaining how many district courts have stated that *Clapper* essentially overruled the *Krottner* decision out of the United States Circuit Court of Appeals for the Ninth Circuit, but other courts found that *Clapper* and *Krottner* are compatible).

146. 628 F. 3d 1139 (9th Cir. 2010).

147. *In re Adobe*, 66 F.Supp.3d at 1214. The district court discussed how the risk hackers will misuse someone's personal information following a security breach is immediate and very real, in contrast to *Clapper*'s "highly attenuated" chain of events. *Id*.

148. *Clapper*, 133 S. Ct. at 1148.

149. *Id.* at 1150.

150. *Green*, 2015 WL 2066531 at *4.

151. *Compare* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 154-55 (2010) (concluding that conventional alfalfa farmers satisfied the injury-in-fact requirement of standing after a government agency deregulated genetically engineered alfalfa because a "significant risk of gene flow to non-genetically-engineered varieties of alfalfa" was a harm the farmers would suffer even if their crops were never contaminated), *with Moyer*, 2014 WL 3511500 at *6 (reasoning that, in light of *Monsanto*, "if a bee's anticipated pollination patterns create[s] a sufficiently imminent risk of injury to alfalfa farmers who fear gene flow from genetically engineered plants in nearby fields, I fail to see how the transfer of information from a data hacker to an identity thief (assuming they are not one and the same) could be deemed an overly attenuated risk of harm.").

152. *See In re Adobe*, 66 F. Supp. 3d at 1214-15 (explaining how, unlike *Clapper*'s highly attenuated chain of events, there is no speculation regarding hackers' intent or ability to misuse information after deliberately targeting the personal information of users on Adobe's servers).

healthcare organizations that reported medical data breaches subsequently experienced cases of medical identity theft.[153] Therefore, the risk of a future injury is not speculative for data security breach victims like district courts have reasoned.[154]

B. Why Medical Security Breaches Require a Different Standard

Medical identity theft is defined as the misuse of someone's personal information to access healthcare.[155] People often find out they are victims of medical identity theft when they are charged for medical services they never received.[156] A medical identity theft victim can establish an actual injury-in-fact for standing purposes as they have already been harmed.[157] However, standing problems arise when victims' personal information has been accessed or acquired without authorization, but not yet misused.[158]

Medical identify theft, the nation's fastest growing crime, has more severe repercussions than financial identity theft.[159] Beyond financial interests, a medical identity theft victim's privacy and health interests are also affected.[160] Medical identity theft victims suffer significantly greater financial consequences than victims of credit card fraud.[161] Entering incorrect health information into the victim's medical records is a potentially dangerous consequence of medical identity

153. *Third Annual Benchmark Study on Patient Privacy & Data Security*, Ponemon Institute, 1, 5, 13 (2012).

154. *See Strautins*, 27 F. Supp. 3d at 877 (noting a 2012 identity fraud study that found victims of data breaches are 9.5 times more likely to suffer from identity theft or identity fraud than people whose information has not been hacked in a data breach).

155. Sullivan, *supra* note 1, at 648.

156. *Id*. at 648.

157. *See* Strautins v. Trustware Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) (discussing how the data breach plaintiffs fail to establish standing with their *increased risk* of identity theft claim, thus implying identity theft is a sufficient injury in fact).

158. *See* Tatiana Melnik, *Data Breach Litigation: Is West Virginia a Trailblazer?* 16 No. 5 J. Health Care Compliance 53, 54 (2014) (stating that data breach cases often fail the injury-in-fact requirement because the fear of becoming an identity theft victim is not an actual injury).

159. *Compare* Rhodes, *supra* note 122, at 20 (labeling medical identity theft "the nation's fastest growing crime"), *and* Ponemon Institute, *supra* note 110, at 8 (noting medical identity theft has increased by 21.7 percent from 2013 to 2014), *with* Ball, *supra* note 93, at 119 (asserting that "[w]hen data breach results in medical identify theft, the results can be even more severe than what occurs in regular identity theft.").

160. Ball, *supra* note 93, at 119. The victim can be billed for services provided to the thief, suffer from exhausted insurance benefits, delays in future services, and suffer from a breach of trust with the victim's medical providers. *Id*.

161. Ponemon Institute, *supra* note 110, at 1. "Sixty-five percent of medical identity theft victims in our study had to pay an average of $13,500 to resolve the crime." *Id*. On the other hand, "the Fair Credit Billing Act (FCBA) limits a consumer's liability to $50 when his or her credit card is used fraudulently." *Id*.

theft.[162] Additionally, victims of medical identity theft often suffer many years down the road because the theft is typically not detected by common reporting methods used by financial identity theft victims.[163] Their problems often continue because the medical records are contained in large medical file databases released to many providers, which makes it difficult for victims to correct every fraudulently altered medical record.[164] In contrast to victims of financial identity theft, very few victims of medical identity theft completely resolve the discrepancies in their medical files.[165]

As medical identity theft is more dangerous to victims and more difficult to fix than financial identity theft, it should be held to a different standard than financial identity theft.[166] Thus, a medical data security breach—or the increased risk of future medical identity theft—should not be analyzed under the *Clapper v. Amnesty International USA*[167] framework that district courts have applied to financial data security breaches.[168]

---

162. Dixon, *supra* note 4, at 6.

163. *Id.* at 17. People often discover they are victims of medical identity theft after receiving collection notices, seeing a credit report, receiving someone else's bills, receiving notification by an insurance fraud investigator or health care provider, insurance coverage denial, or the most catastrophic—during a medical emergency. *Id*. at 31-33.

164. Sullivan, *supra* note 1, at 656. While HIPAA provides an individual with the ability to amend his or her medical records, there are problems. Dixon, *supra* note 4, at 40-41. When medical information is sent from one provider or insurer to another, the latter does not have to correct the medical information received, and not all copies of the medical file (such as records used in labs) are always corrected. *Id*. at 40-41.

165. *Compare Javelin Study Finds Identity Fraud Reached New High in 2009, But Consumers Are Fighting Back*, JAVELIN STRATEGY & RESEARCH, https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail (determining it takes a victim of financial identity theft approximately twenty-one hours to resolve his claim), *with* PONEMON INSTITUTE, *supra* note 110, at 1 (concluding that only ten percent of medical identity theft victims in the study reported "a completely satisfactory conclusion of the incident.").

166. *Compare* Rinehart-Thompson, *supra* note 99, at 75 (stating that medical identity theft can lead to potentially life-threatening treatment), *and* Dixon, *supra* note 4, at 9 (explaining how medical identity theft is hard because the victims cannot detect the errors as easily as financial identity theft victims, nor can they correct their medical files as well), *and* Rhodes, *supra* note 122, at 21 (stating that the problem with medical identity theft is that "false medical information lives forever . . . ."), *with Strautins*, 27 F. Supp. 3d at 876 (determining an increased risk of identity theft is not sufficient to meet the certainly impending standard for standing).

167. 133 S. Ct. 1138 (2013).

168. *Compare* Sullivan, *supra* note 1, at 666 (contending that it is difficult for medical identity theft victims to recover for their problems, so litigation may be an option, but victims are limited in what causes of action they can even bring), *and* Dixon *supra* note 4, at 5-6 (explaining the dangers involved with medical identity theft), *and Remijas*, 794 F.3d at 694 (noting that it is important to not overread *Clapper* in the data breach context), *with Peters*, 74 F. Supp. 3d at 855 (reasoning "[u]nder *Clapper*, Peters must at least plausibly establish a 'certainly impending' . . . risk" to satisfy the injury-

C. ALTERNATIVE

Some experts have argued that medical identities are more valuable to criminal hackers because of the comprehensive data in a stolen electronic medical record.[169] Further, healthcare providers are one of the leading personal data compilers.[170] The current system requires all individuals to be directly informed if their protected health information has been involved in a data breach.[171] However, there is no federal private right of action for medical identity theft, nor is there any federal statutory relief for victims whose medical information is breached but not yet misused.[172] Medical security breaches will continue to grow in number because the complex electronic health record systems give hackers access to unlimited medical information.[173] Medical data breach victims continue to suffer without having their injuries redressed because state law recourses are incomplete and there is no federal statutory private right of action for a medical data breach.[174] Thus, when data breach victims attempt to use the judicial process, they are now faced with federal courts' post-*Clapper* trend to dismiss data breach claims for lack of standing because their injuries are speculative.[175] However, the potentially devastating harm medical data breach victims could suffer, if their information is actually misused in a subsequent medical identity theft, requires a lower standard to establish standing so victims can have the merits of their claims heard.[176] Therefore, since the political branches have not cre-

---

in-fact requirement for standing, and her risk of future identity theft did not meet this standard).

169. Terry, *supra* note 106, at 72.

170. Sullivan, *supra* note 1, at 648.

171. Dixon, *supra* note 4, at 44.

172. *See* Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 468-69 (D.N.J. 2013) (stating how HIPAA does not create a private right of action after the data breach plaintiff tried to establish her standing injury as a violation of HIPAA).

173. *Compare* Dixon, *supra* note 4, at 9-10 (discussing challenges faced by medical identity theft victims because of the increased digitization of medical records in recent years), *with* PONEMON INSTITUTE, *supra* note 110, at 9 (explaining how medical identity theft has increased by 21.7 percent from 2013 to 2014, resulting in 481,657 new cases).

174. *Compare* Dixon, *supra* note 4, at 10-11 (noting how medical identity theft victims are "falling through several existing gaps [because] financial identity theft experts are seldom experts in the federal privacy rule known as HIPAA or in the complexities of the medical care treatment and payment systems . . . [t]he Federal Trade Commission ("FTC"), which has studied financial identity theft, is not responsible for addressing medical issues."), *with* Sullivan, *supra* note 1, at 667 (noting how state laws do not fully encompass medical identity theft).

175. *See* Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *3 (E.D. La. May 4, 2015) (stating that most courts have dismissed data breach claims because an increased risk of future identity theft does not meet *Clapper*'s certainly impending standard to establish standing).

176. *Compare* In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (asserting how *Clapper*'s standing analysis revolved around the sensitive topic of political branches violating the Constitution, making it unusually rigorous), *and*

ated a statutory private right of action for medical data breach victims, the judicial branch should subject medical data breaches to the substantial risk of harm standard—rather than the certainly impending standard applied by the *Clapper* court.[177]

Standing based on a future harm requires a certainly impending harm or a substantial risk of harm.[178] *Clapper* did not overrule the line of cases that established standing based on substantial risk of harm would occur.[179] While *Clapper* relegated its reference to the substantial risk standard to a footnote, *Monsanto Co. v. Geertson Seed Farms*[180] discussed the substantial risk standard in its standing analysis.[181] Unlike the respondents in *Clapper*, medical data breach victims have evidence to support the notion that an increased threat of future identity theft establishes standing.[182] Additionally, waiting for a data breach to materialize into identity theft creates more difficulty

---

Rhodes, *supra* note 122, at 21 (stating that "[m]edical identity theft could have life threatening consequences"), *with* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (concluding that in light of *Clapper*, Peters' heightened risk of future identity theft does not meet the injury-in-fact requirement).

177. *Compare* Sullivan, *supra* note 1, at 666 (noting how in theory, vigorous judicial remedies would incentivize "health care providers to do a better job of preventing identity theft from occurring in the first place"), *with* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (inferring that plaintiffs have established a substantial risk of harm as victims of the Neiman Marcus data breach, to survive a motion to dismiss).

178. In re Zappos.com, Inc., No. 3:12-cv-00325-RCJ-VPC, 2015 WL 3466943, at *3 (D. Nev. June 1, 2015) (citing Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014)); *see also Peters*, 74 F. Supp. 3d at 855 (stating a cognizable injury requires a plausible certainly impending risk or substantial risk that the identity theft will occur).

179. *In re Adobe*, 66 F. Supp. 3d at 1213; *see also* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153-56 (2010) (determining traditional alfalfa farmers had standing to challenge the use of a genetically engineered alfalfa herbicide because there was a substantial risk that the gene flow from the genetically modified alfalfa herbicide would harm the traditional alfalfa crops); *but see Remijas*, 794 F.3d at 694 (noting that *Clapper* stated that mitigation expenses are insufficient as an injury for standing when the harm is not imminent).

180. 561 U.S. 139 (2010).

181. *See Monsanto*, 561 U.S. at 153-54 (reasoning that the deregulation of the genetically engineered alfalfa herbicide creates a substantial risk of injury to traditional alfalfa farmers because the traditional alfalfa farmers must test their crops for contamination in order to continue advertising their product as non-genetically-engineered alfalfa and the risk of gene flow requires the farmers to protect their traditional alfalfa crops from contamination).

182. *Compare Clapper*, 133 S. Ct. at 1154 (noting how respondents presented "no concrete evidence to substantiate their fears, but instead rest[ed] on mere conjecture about possible governmental actions."), *with Monsanto*, 561 U.S. at 154-155 (explaining that traditional alfalfa farmers established standing by presenting evidence of increased costs to test for potential contamination), *and Third Annual Benchmark Study on Patient Privacy & Data Security*, PONEMON INSTITUTE, 1, 5, 13 (2012) (finding that 94% of healthcare organizations surveyed suffered at least one data breach the past two years, 52% of the organizations subsequently had cases of medical identity theft, and 39% of the healthcare providers with medical identity theft incidents reported the theft "resulted in inaccuracies in the patient's medical record . . . .").

establishing the fairly traceable requirement of standing.[183] The dangerous and perpetual problems associated with medical identity theft, the fastest growing crime in the United States, compels lower standing barriers for medical data breach victims as a way to help deter future hackers and force healthcare providers to launch stricter preventative measures.[184]

D. Objections and Rebuttal

Regarding the proposed alternative to apply the substantial risk standard to the injury-in-fact requirement of standing in medical data breach claims, it is first unclear what the difference is between the certainly impending and the substantial risk standards.[185] The United States Supreme Court in *Clapper v. Amnesty International USA*[186] declined to explain the difference between a risk of future harm that is certainly impending and a substantial risk of future harm.[187] Additionally, lower federal courts have refrained from clarifying the difference between the two standards in the post-*Clapper* era, but the substantial risk standard is arguably more lenient than the certainly impending standard.[188] Second, while the substantial risk standard can establish standing, critics may argue a threat of

183. *Remijas*, 794 F.3d at 693. The court reasoned that customers who had their credit card information hacked should not have to wait until the hackers commit identity theft in order to have standing. *Id*.

184. *Compare* Ponemon Institute, *supra* note 110, at 1-2 (discussing the dangers, complexities, reputational fears, and financial costs associated with medical identity theft), Steve Lohr, *The New Hacker Economics*, New York Times (2008) (explaining a recent study that found medical data sells on the black market for $150 to $200, while credit card numbers and bank account pins only sell for $10 to $20), Sullivan, *supra* note 1, at 666 (noting "a robust set of judicial remedies would create a strong incentive; for health care providers to do a better job of preventing identity theft from occurring in the first place"), *and* Rhodes, *supra* note 122, at 20 (stating "medical identity theft has been labeled as the nation's fastest growing crime."), *with Remijas*, 794 F.3d at 693 (determining that the data breach victims had a substantial risk of future identity theft which satisfied the injury-in-fact requirement for standing).

185. *See* Green v. eBay Inc., No. 14-1688, 2015 WL 2066531, at *5, n. 55 (E.D. La. May 4, 2015) (stating that "[t]o the extent there is any relevant difference between the 'certainly impending' and 'substantial risk' standards, Plaintiff has not demonstrated either.").

186. 133 S. Ct. 1138 (2013).

187. *See* In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1217, n.7 (N.D. Cal. 2014) (stating that "[t]he *Clapper* Court declined, however, to determine whether a 'substantial' risk of future harm is meaningfully different from a 'certainly impending' risk of future harm.")

188. *Compare* Hedges v. Obama, 724 F.3d 170, 196 (2d Cir. 2013), *cert. denied*, 134 S. Ct. 1936 (2014) (discussing how the Supreme Court in *Clapper* "did not explain when [the substantial risk] standard might apply . . . ."), *with* Bradford C. Mank, *Clapper v. Amnesty International: Two or Three Competing Philosophies of Standing Law?*, 81 Tenn. L. Rev. 211, 217 (2014) (stating that the substantial risk standard "may be more lenient than" *Clapper*'s certainly impending standard).

possible identity theft is not a *substantial* risk.[189] A nineteen percent chance of financial identity theft following a financial data breach may not be a substantial risk for financial data breach victims; however, a fifty-two percent chance of medical identity theft after a healthcare organization has experienced a medical data breach is a substantial risk of harm for patients whose information was stolen.[190] In 2014, the Ponemon study further concluded that it costs victims of medical identity theft approximately $13,500 to resolve the identity theft ramifications.[191]

Alleging a possible future injury does not sufficiently meet the post-*Clapper* certainly impending standing requirements.[192] However, if courts do not establish a different standard for medical data breach standing, medical data breach victims, by the nature of their claim, will be in limbo between a possible future injury and a certainly impending injury.[193] This is problematic because a medical identity theft following a medical data breach has cascading, dangerous effects.[194] Applying the substantial risk of harm standard to medical data breaches would allow victims to survive a motion to dismiss and have the merits of their cases heard in court.[195] By allowing medical

189. *See* In re SAIC Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (noting that because only nineteen percent of data breach victims ultimately suffered from identity theft, the data breach victims failed to establish standing under the substantial risk standard).

190. *Compare In re SAIC*, 45 F. Supp. 3d at 26 (noting that because only nineteen percent of data breach victims ultimately suffered from identity theft, the data breach victims failed to establish standing under the substantial risk standard), *with Third Annual Benchmark Study on Patient Privacy & Data Security*, PONEMON INSTITUTE, 1, 13 (2012) (finding that ninety-four percent of healthcare organizations surveyed suffered at least one data breach in the last two years, and fifty-two percent of those healthcare organizations subsequently experienced at least one medical identity theft incident).

191. *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data*, PONEMON INSTITUTE, 1, 2 (2015).

192. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

193. *Compare* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (stating that *Clapper* "did not jettison the 'substantial risk' standard"), *and In re SAIC*, 45 F. Supp. 3d at 26 (noting that the data breach victims could theoretically establish standing if the risk of harm were substantial), *with* Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 856 (S.D. Tex. 2015) (determining that victims of a data breach at St. Joseph Regional Health Center lacked standing because their claims were based on an increased risk of future identity theft).

194. *See* Reba L. Kieke, *Although a Relatively New Risk Area, Medical Identity Theft Should Not Be Taken Lightly*, 11 NO. 1 J. HEALTH CARE COMPLIANCE 51, 53 (2009) (explaining that "AHIMA has created a diagram . . . which demonstrates how medical identity theft affects an individual and his or her health care from the initial theft to corrupted health records.").

195. *Compare Remijas*, 794 F.3d at 693 (explaining that "[a]t this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal consumers' private information?"), *with Clapper*, 133 S. Ct. at 1150

data breach victims to reach the merits of their case, hospitals and other health care providers will hopefully establish more rigorous mechanisms to combat medical identity theft from ensuing in the first place, thereby decreasing the number of medical data breaches in the future.[196] Therefore, the increase in medical identity theft in recent years and the severity of its ramifications necessitates a well-rounded approach, including judicial assistance.[197]

The original purpose of the standing doctrine was to protect the Constitution's separation of powers.[198] Denying the right of adjudication to medical data breach victims does not serve the original purpose of standing.[199] Additionally, allowing medical data breach victims to meet the injury-in-fact requirement of standing through the substantial risk standard will not mean all healthcare provider systems automatically lose in litigation because the victims still must prove the likelihood of possible medical identity theft during the discovery process to recover.[200] Even though medical data breach victims have a long road to recovery—due to the magnitude of the threatened harm they face—they deserve to have the merits of their claims adjudicated.[201]

IV. CONCLUSION

While *Clapper v. Amnesty International USA*[202] may have correctly found that the respondents lacked standing to challenge the

n.5 (stating that plaintiffs do not have "to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur . . . .").

196. *See* Sullivan, *supra* note 1, at 665 (discussing how there are no federal remedies offered to medical identity theft victims and "a robust set of judicial remedies would create a strong incentive for health care providers to do a better job of preventing identity theft from occurring in the first place.").

197. *See* Mike Miliard, *Healthcare to be 'plagued' by data breaches in 2015*, HEALTHCARE IT NEWS, 2014 (quoting Ann Patterson, the senior vice president of the Medical Identity Fraud Alliance, who stated, "[t]here is no single solution for fraud prevention, meaning we must take a collaborative approach to solving the issue.").

198. Allen v. Wright, 468 U.S. 737, 752 (1984).

199. *See* In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014) (stating that plaintiffs need to only plausibly allege that they have standing at the motion to dismiss stage).

200. *See Remijas*, 794 F.3d at 694 (recognizing that the data breach victims may not be able to provide a sufficient factual basis to support their claim of an increased risk of identity theft, but they have "no such burden at the pleading stage").

201. *Compare Remijas*, 794 F.3d at 693 (stating that there was a substantial risk of harm following a data breach to confer standing on the data breach victims), *and In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d at 1158-59 (determining data breach victims had standing to survive the motion to dismiss stage because they have alleged an injury-in-fact), *with Peters*, 74 F. Supp. 3d at 854 (reasoning that plaintiff's increased risk of identity theft was not certainly impending and as a result, did not establish standing).

202. 133 S. Ct. 1138 (2013).

constitutionality of the Foreign Intelligence Surveillance Act,[203] lower federal district courts should be hesitant to apply *Clapper*'s standing analysis to data breach claims.[204] This is especially pertinent for medical data breach victims because the possible future injury of medical identity theft is too dangerous to shut the judicial door on victims from having the merits of their claims heard.[205] As medical identity theft is the nation's fastest growing form of identity theft, its consequences require the federal courts to apply a lower standing standard to medical data breaches, in hopes that healthcare providers will create stricter preventative measures to avoid future medical data breaches.[206] Therefore, instead of applying *Clapper*'s certainly impending standard to medical data breach claims, federal courts should apply the substantial risk of harm standard.[207] While critics may argue the substantial risk of harm standard is hardly different from the certainly impending standard, and federal courts have scarcely applied it, the standard is still good law and the dangers associated with medical identity theft require judicial action as part of a collaborative effort to solve this problem.[208]

Claire Wilka—'17

203. 50 U.S.C. § 1881a (2015).
204. *See supra* notes 123-153 and accompanying text.
205. *See supra* notes 155-168 and accompanying text.
206. *See supra* notes 169-184 and accompanying text.
207. *See supra* notes 169-184 and accompanying text.
208. *See supra* notes 185-201 and accompanying text.