NEW YORK LAW SCHOOL

NYLS Law Review

Volume 63
Issue 3 *Spotlight on Select Student Scholarship*

Article 2

April 2019

Chambliss v. CareFirst, Inc.

Sarah Fucci

VOLUME 63 | 2018/19

SARAH FUCCI

Chambliss v. CareFirst, Inc.

63 N.Y.L. Sch. L. Rev. 321 (2018–2019)

ABOUT THE AUTHOR: Sarah Fucci is the Executive Notes & Comments Editor of the 2018–2019 *New York Law School Law Review*, J.D. candidate, New York Law School, 2019.

"Your identity is your most valuable possession."[1] Imagine if this vital aspect of who you are was taken from you and there was nothing you could do to protect it. Identity theft is not a hypothetical fear—it is a reality that approximately 16.7 million Americans faced in 2017.[2] The healthcare industry is a particularly "attractive target" for hackers.[3] The potential harm can include financial loss; credit troubles; erroneous medical records; loss of federal or state benefits; and even criminal implications, such as false arrest.[4] With technological advancements outpacing security measures and instances of identity theft on the rise, you might be more at risk than you think.[5]

In *Chambliss v. CareFirst, Inc.*, the United States District Court for the District of Maryland considered whether customers of CareFirst health insurance, whose information was stolen as a result of a data breach, had Article III standing to bring their putative class action.[6] If successful, CareFirst's customers would have been able to litigate their various tort, negligence, and statutory claims in federal court.[7] Instead, the court dismissed their claims, finding that the *Chambliss* plaintiffs failed to produce evidence sufficient to confer standing.[8]

---

1. The Incredibles (Pixar Animation Studios 2004).

2. Al Pascual, Kyle Marchini & Sarah Miller, *2018 Identity Fraud: Fraud Enters a New Era of Complexity*, Javelin (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity; *see also* Ben Keylor, *What Are Your Odds of Getting Your Identity Stolen?*, IdentityForce: Identity & Privacy (Jan. 2, 2018), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (discussing the likelihood of becoming a victim of identity theft).

3. Matthew Goldstein & Reed Abelson, *Up to 1.1 Million Customers Could Be Affected in Data Breach at Insurer CareFirst*, N.Y. Times (May 20, 2015), https://www.nytimes.com/2015/05/21/business/carefirst-discloses-data-breach-up-to-1-1-million-customers-affected.html?_r=0; *see also* Paige Schaffer, *Data Breaches on the Rise: How Healthcare Organizations Can Protect Against Medical Identity Theft*, Healthcare Analytics News (July 3, 2018), https://www.hcanews.com/news/data-breaches-on-the-rise-how-healthcare-organizations-can-protect-against-medical-identity-theft ("[H]ealth system cybersecurity is, like in many other industries, inadequate.").

4. *What Are the Effects of Identity Theft?*, TransUnion: Identity Protection (Oct. 12, 2016), https://www.transunion.com/blog/identity-protection/what-are-the-effects-of-identity-theft. The Federal Trade Commission (FTC) has recognized that "[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance," and can even "file a tax return in your name and get your refund." Fed. Trade Comm'n, *Warning Signs of Identity Theft*, IdentityTheft.gov, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Mar. 28, 2019).

5. *See* Rajiv Leventhal, *Report: In New Digital Environments, Data Breaches Are the Norm*, Healthcare Informatics (Jan. 30, 2018), https://www.healthcare-informatics.com/news-item/cybersecurity/report-new-digital-environments-data-breaches-are-norm ("[W]hile times have changed with respect to technological advancements, security strategies have not . . . leaving customer data . . . severely at risk."); *see also* Keylor, *supra* note 2 ("Unfortunately, even though people may think [identity theft] is somewhat rare, identity theft statistics show that your chances of being affected might be much higher than you think.").

6. 189 F. Supp. 3d 564, 566–67 (D. Md. 2016).

7. *Id.* at 567.

8. *Id.* at 571.

On May 20, 2015, the *New York Times* reported that CareFirst, a Maryland health insurance provider, announced that a recent hack compromised the confidential personal information of over one million of its customers,[9] including their names, birth dates, e-mail addresses, and subscriber identification numbers.[10] As a health insurance provider, CareFirst was likely an attractive, "soft target" for hackers[11]: Like most in the healthcare industry, CareFirst's computers and data storage devices were not encrypted.[12]

After learning of the breaches, CareFirst customers ("Plaintiffs") brought a class action against CareFirst.[13] In response, CareFirst filed a motion to dismiss for lack of subject matter jurisdiction, arguing that Plaintiffs lacked standing.[14] To establish standing, a plaintiff must show that they have suffered an "injury in fact," which is an invasion of a legally protected interest that is both (1) concrete and particularized and (2) actual or imminent, not conjectural or hypothetical.[15] Plaintiffs argued that an increased risk of future harm—specifically, identity theft—satisfied the requisite injury for the court to have jurisdiction to adjudicate their claims.[16] Ultimately, the court held that Plaintiffs failed to meet their burden and granted CareFirst's motion to dismiss the case for lack of subject matter jurisdiction.[17]

9. Goldstein & Abelson, *supra* note 3.

10. *Chambliss*, 189 F. Supp. 3d at 567. A subscriber identification number is the number associated with a customer's particular health insurance plan. *What Is a Subscriber ID Number for Health Insurance?*, Health Ins. Providers, https://www.healthinsuranceproviders.com/what-is-a-subscriber-for-health-insurance (last updated Apr. 10, 2017).

11. *See* Goldstein & Abelson, *supra* note 3; *see also* Erin McCann, *Anthem Hack: 'Healthcare Is a Target,'* Healthcare IT News (Feb. 6, 2015), https://www.healthcareitnews.com/news/anthem-hack-healthcare-target?mkt_tok=3RkMMJWWfF9wsRols6rIZKXonjHpfsX56eoqUaW%2BlMI%2F0ER3fOvrPUfGjI4CRMpjI%2BSLDwEYGJlv6SgFQ7LHMbpszbgPUhM%3D (explaining that healthcare organizations are "soft targets" because "historically, [they] have invested less in [information technology], including security technologies and services than other industries," and are thus more vulnerable to cyberattacks).

12. Class Action Complaint at 4, *Chambliss*, 189 F. Supp. 3d 564 (No. RDB-15-2288).

13. Plaintiffs, represented by litigants Pamela Chambliss and Scott Adamson, asserted five claims arising under federal and Maryland law: negligence; breach of implied contract; unjust enrichment; declaratory judgment pursuant to 28 U.S.C. § 2201 (2016); and violation of the Maryland Personal Information Protection Act, Md. Code Ann., Com. Law §§ 14-3501–3508 (West 2018). *Chambliss*, 189 F. Supp. 3d at 567; Class Action Complaint, *supra* note 12, at 6–7.

14. *Chambliss*, 189 F. Supp. 3d at 568. A motion to dismiss for lack of subject matter jurisdiction "challenges a court's authority to hear the matter brought by a complaint." *Id.* CareFirst also filed a motion to dismiss for failure to state a claim, but the *Chambliss* court only addressed CareFirst's jurisdictional objections. *Id.*

15. *Id.* at 569 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). As the party seeking federal jurisdiction, Plaintiffs had the burden of establishing standing, which also requires showing that the alleged injury is fairly traceable to the defendant and is likely to be redressed by a favorable decision. *Id.* at 569. This Case Comment addresses the injury-in-fact requirement of standing.

16. *See Chambliss*, 189 F. Supp. 3d at 569. Plaintiffs argued three other theories of injury that were considered by the court, *see id.*, but are not discussed in this Case Comment.

17. *Id.* at 572–73.

In reaching its conclusion, the court looked to the "certainly impending" test laid out in 2013 by the United States Supreme Court in *Clapper v. Amnesty International USA*,[18] and stated that in cases involving risk of future harm, "the threatened injury must be *certainly impending* to constitute an injury in fact. . . . In other words, there must be a '*substantial risk*' that the harm will occur."[19] The *Chambliss* court reasoned that even though Plaintiffs' information was stolen, under *Clapper*, the alleged injury was not "certainly impending" because their theory of future harm "depend[ed] on a chain of assumptions that must occur before the harm materializes," namely, "on the actions of an unknown independent third party."[20] Finding it unclear whether, when, or how a hacker would use their stolen information to cause future harm, the court held that Plaintiffs' alleged injury was too speculative to be "certainly impending" and dismissed their case.[21]

This Case Comment contends that the *Chambliss* court incorrectly analyzed the injury-in-fact requirement of Article III standing, thus denying Plaintiffs the ability to proceed on the merits of their claims. First, the court incorrectly intertwined the "certainly impending" and "substantial risk" tests, which are actually two separate analyses. Second, the court failed to recognize that *Clapper*'s overly rigorous future risk of harm analysis is inapplicable to data breach cases. Finally, the court's decision sets a precedent that essentially forces customers whose information has been compromised to wait until their stolen identity is wrongfully used before they can sue in federal court.

First, the *Chambliss* court failed to distinguish the "certainly impending" test from the "substantial risk" test when analyzing whether future harm satisfies the injury-in-fact requirement of Article III standing. To constitute an injury in fact, the injury must be "actual or imminent, not conjectural or hypothetical."[22] Thus, in cases when harm has not yet occurred, for harm to be "imminent" it must be "certainly impending," or there must be a "substantial risk that the harm will occur."[23] The "certainly impending" and "substantial risk" tests are separate and distinct: As the Court in *Clapper* acknowledged when applying the former, "[o]ur cases do not uniformly require plaintiffs 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 . . . ."[24] But the Supreme Court has used

18. 568 U.S. 398 (2013).

19. *Chambliss*, 189 F. Supp. 3d at 569 (first quoting *Clapper*, 568 U.S. at 401; then quoting Susan B. Anthony List v. Driehaus, 57. U.S. 149, 158 (2014)).

20. *Id.* at 570.

21. *Id.* at 570–72.

22. *Driehaus*, 57. U.S. at 158 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

23. *See Clapper*, 568 U.S. at 409, 414 n.5.

24. *Id.* (emphasis added); *see also* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015) (stating that the Supreme Court "did not jettison the 'substantial risk' standard" when it applied the "certainly impending" test in a case involving a high degree of speculation of future harm); Arthur R. Vorbrodt, Clapper *Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison*, 73

both standards in different contexts,[25] leading to some mixed applications among the lower courts.[26]

Nonetheless, the "certainly impending" test is a stricter standard than the "substantial risk" test.[27] In light of this fact, some lower courts have recognized that the lower, "substantial risk" standard—or something akin to it—is more appropriate for data privacy cases. For example, in 2010 the U.S. Court of Appeals for the Ninth Circuit in *Krottner v. Starbucks Corp.* granted standing based on "a credible threat of harm" from a stolen laptop containing sensitive personal information.[28] The court found that the plaintiffs' increased risk of identity theft was sufficient to constitute injury in fact, even though no theft had yet occurred.[29]

More recently, the Seventh Circuit in *Remijas v. Neiman Marcus Group* held that the alleged future threat of identity theft created a substantial risk of harm and was therefore sufficient to constitute an injury in fact.[30] *Remijas* involved a data breach at the department store Neiman Marcus.[31] Neiman Marcus confirmed the breach and notified customers that their payment card account information, but no other personal information, had been potentially exposed.[32] Nonetheless, the court found the risk of future injury "substantial" because the hacker most likely intended to someday use the breached information to the detriment of the victims.[33]

Wash. & Lee L. Rev. Online 61, 73 (2016) ("The [certainly impending and substantial risk] standards are not interchangeable and may possibly lead to different outcomes.").

25. *Compare* Whitmore v. Arkansas, 495 U.S. 149, 157–58 (1990) (employing the "certainly impending" standard when denying third-party standing to challenge the validity of a defendant's death sentence), *with* Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153–54 (2010) (granting standing based on the "substantial risk" of contamination from a neighboring farmer's genetically modified crop).

26. *See, e.g.*, Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 878 n.11 (N.D. Ill. 2014) ("[T]he import of *Clapper* for standing analysis . . . is a question on which reasonable minds may differ."); Vorbrodt, *supra* note 24, at 87 ("Many district courts interpret *Clapper* as a large hurdle for data breach claims relying on imminent injury; others interpret *Clapper* to tighten constitutional standing altogether.").

27. *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017) (quoting *Clapper* when concluding that the plaintiffs' risk of future harm was too speculative to be "certainly impending," and that they "also failed to satisfy the 'lesser standard' of 'substantial risk' of future harm"); *see also* Joseph J. Vacek, *The Next Frontier in Drone Law: Liability for Cybersecurity Negligence and Data Breaches for UAS Operators*, 39 Campbell L. Rev. 135, 159 (2017) (stating that *Clapper* imposes "stricter requirements" for standing than the "substantial risk standard").

28. 628 F.3d 1139, 1143 (9th Cir. 2010).

29. *Id.*

30. 794 F.3d 688, 693–94 (7th Cir. 2015).

31. *See id.* at 689.

32. *Id*. at 690.

33. *See id.* at 693 ("Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."); *see also* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966–67 (7th Cir. 2016). *Lewert* involved a data breach at thirty-three P.F. Chang restaurants, compromising customers' debit and credit card information. *Id.* at 965. The court accepted the plaintiffs' future risk of harm theory based on the analysis from *Remijas*. *Id.*

Here, the *Chambliss* court conflated the two standards by stating that "the threatened injury must be *certainly impending* to constitute an injury in fact. . . . *In other words*, there must be a *substantial risk* that the harm will occur."[34] The phrase "in other words" demonstrates that the court incorrectly took the "certainly impending" and "substantial risk" tests to be one and the same.[35] In its analysis, the court omitted any reference to the substantial risk of harm theory, reasoning that it was "not clear *whether* future harm from a data security breach will materialize, [and] *uncertain when* such harm will occur"—an analysis that seeks literal certainty.[36]

Since the court ignored relevant case law and failed to analyze the two tests separately, it incorrectly found that Plaintiffs' future threat of identity theft was insufficient to establish imminent injury. Had the court followed the examples set forth in *Krottner* and *Remijas*, it would have completed a separate analysis under the more relaxed "substantial risk" test and found that personal information, once stolen, substantially increases a person's risk of identity theft and is therefore imminent, satisfying the injury-in-fact requirement of Article III standing.

Second, even if the stricter, "certainly impending" test from *Clapper* was appropriate, the *Chambliss* court applied it in an overly rigorous manner, resulting in an improper future threat of harm analysis. *Clapper* involved a constitutional challenge of a newly enacted statute that allowed the federal government to engage in surveillance of non-U.S. citizens located outside the United States.[37] Before proceeding with an "especially rigorous" standing inquiry, the Court acknowledged its own reluctance to grant standing when called upon "to review actions of the political branches in the fields of intelligence gathering and foreign affairs."[38] The Court described at length a series of five highly speculative events involving multiple parties that would have to take place before the alleged future injury could occur,

---

34. Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564, 569 (D. Md. 2016) (second emphasis added) (internal quotations omitted) (first quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013); then quoting Susan B. Anthony List v. Driehaus, 57. U.S. 149, 158 (2014)).

35. According to Merriam-Webster, the phrase "in other words" is "used to introduce a statement that repeats what has been said in a different and usually a simpler or more exact way." *In Other Words*, Merriam-Webster.com, https://www.merriam-webster.com/dictionary/in%20other%20words (last visited Mar. 29, 2019).

36. *Chambliss*, 189 F. Supp. 3d at 570 (quoting *In re* SuperValu, Inc., No. 14-MD-2586 ADM/TNL, 2016 U.S. Dist. LEXIS 2592, at *12 (D. Minn. Jan. 7, 2016), *aff'd in part, rev'd in part sub nom.* Alleruzzo v. Supervalu, Inc., 870 F.3d 763 (2017)). An analysis involving literal certainty is an analysis under the "certainly impending" test, not the "substantial risk" test. *See supra* text accompanying notes 24–27.

37. *Clapper*, 568 U.S. at 401. The respondents, a group of attorneys and human rights, labor, legal, and media organizations, alleged that the statute violated the constitutional rights of their clients or constituents with whom they were required to engage in sensitive international communications and were likely targets of the surveillance. *Id.* at 406–07.

38. *See id.* at 408–09 ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional. . . . [W]e have often found a lack of standing in [such] cases . . . .") (internal quotations omitted).

then used this "highly attenuated chain of possibilities" to determine that the alleged future injury was not certainly impending to amount to an injury in fact.[39]

However, courts have recognized that the *Clapper* Court did not intend to replace its well-established "certainly impending" test with a more rigorous approach; rather, it was the "sensitive context" of alleged constitutional violations that led to the Court's "unusually rigorous" analysis of future harm.[40] Courts that have properly recognized the unusual context in which *Clapper* was decided have found the future threat of identity theft sufficient to satisfy the injury-in-fact requirement of Article III standing.[41] In such cases, a crucial component in determining whether future harm is certainly impending is whether information has actually been stolen.[42]

For example, in 2014, the Northern District of California found it "certainly impending" that the plaintiffs' personal data would be misused by hackers after a data breach of Adobe's servers.[43] Adobe announced that hackers were able to access the personal information of millions of customers, including names, login IDs, passwords, credit and debit card numbers, and mailing and e-mail addresses.[44] The court reasoned that "in contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored under [the law at issue], here, there was no need to speculate as to whether Plaintiffs' information

39. *Id.* at 410. The respondents could only speculate as to whether the following five events would happen: (1) whether the government would target communications to which respondents were parties; (2) if so, whether the government would invoke its authority under the statute to conduct surveillance rather than use other methods; (3) whether the court charged with enforcing the statute's Fourth Amendment safeguards would authorize the surveillance; (4) whether the government would succeed in acquiring the communications of respondents' foreign contacts; and (5) whether the respondents would be parties to the communications intercepted. *Id.*

40. *See In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1213–14 (N.D. Cal. 2014) ("*Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result."); *see also* Vorbrodt, *supra* note 24, at 74 (arguing that *Clapper* did nothing to alter the "well-established case law regarding imminent injury in data breach lawsuits").

41. *See, e.g.*, Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (finding the allegations of future identity theft satisfied the injury-in-fact requirement and recognizing that it was "important not to overread *Clapper*," since it addressed "speculative harm based on something that may not even have happened to some or all the plaintiffs"); *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d at 1214–15 (distinguishing *Clapper* and finding the future threat of identity theft sufficient to establish standing).

42. *See, e.g.*, Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967 (7th Cir. 2016) (holding that plaintiffs' alleged injuries were not mere allegations of possible future injury "because their data has actually been stolen"); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (noting that the "common denominator" among data breach cases is that "data actually has been accessed through a security breach"); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) ("Were Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would have been stolen at some point in the future—we would find the threat far less credible.").

43. *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d at 1220.

44. *Id.* at 1206.

has been stolen and what information was taken."[45] Acknowledging that injury would "be more imminent" if the plaintiffs alleged that their information had already been misused, the court nonetheless granted standing, because "why would hackers target and steal personal customer data if not to misuse it?"[46]

On the heels of *Adobe,* the Seventh Circuit in *Remijas* found that *Clapper* did not foreclose the risk of future harm as a theory of injury for Article III standing, and distinguished *Clapper* by emphasizing that the *Clapper* plaintiffs failed to show that their communications were actually intercepted by the government.[47] While the *Remijas* court granted standing based on the "substantial risk" test, the court recognized that "it was important not to overread *Clapper*" since it addressed "speculative harm based on something that may not even happen to some or all of the plaintiffs."[48]

Here, by failing to recognize *Clapper*'s unusually rigorous approach, the *Chambliss* court wrongly focused on the type of data stolen and the fact that it had not yet been misused. Adopting *Clapper*'s demanding "chain of possibilities" template, the court explained that a hacker must (1) read, copy, and understand the personal information; (2) intend to commit future criminal acts by misusing the information; and (3) be able to use such information to the detriment of another by making unauthorized transactions in another's name.[49] In so doing, the court overlooked the crucial point recognized by its sister circuits: *Clapper*'s rigorous imminent injury analysis is inappropriate for data breach cases.[50] Further, while the *Chambliss* data breach did not involve financial information, the future threat of identity theft is still a real concern for victims: Stolen personal health insurance information can be used by hackers to obtain expensive medical services, to fraudulently acquire government benefits, or to perpetuate more thefts.[51]

---

45. *Id.* at 1214–15 (internal citation omitted).

46. *Id.* at 1215–16.

47. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (2015) ("In *Clapper*, the Supreme Court decided that human rights organizations did not have standing . . . because they could not show that their communications with suspected terrorists *were* intercepted by the government. The plaintiffs only suspected that such interceptions might have occurred. This, the Court held, was too speculative to support standing.").

48. *Id.* at 694.

49. Chambliss v. CareFirst, Inc., 189 F. Supp. 3d 564, 570 (D. Md. 2016).

50. *See Remijas*, 794 F.3d at 693 (stating that in data breach cases, "a substantial risk will sometimes suffice to support Article III standing"); Vacek, *supra* note 27, at 159 (noting that to apply *Clapper*'s "more stringent requirement" in data breach cases "would effectively bar most data breach plaintiffs from proceeding").

51. *See* Class Action Complaint, *supra* note 12, at 4–5; *see also Facts + Statistics: Identity Theft and Cybercrime*, Ins. Info. Inst., http://www.iii.org/fact-statistic/identity-theft-and-cybercrime (last visited Mar. 29, 2019) ("New account fraud occurs when a thief opens a credit card or other financial account using a victim's name and other stolen personal information."); OccupyTheWeb, *Extracting Data from Online Databases Using Sqlmap*, WonderHowTo: Null Byte (Jan. 28, 2014, 2:07 PM), https://null-byte.wonderhowto.com/how-to/hack-databases-extracting-data-from-online-databases-using-

Moreover, allegations of data misuse are not necessary to establish standing. A "common denominator" in determining standing among data breach cases is whether "the data actually had been accessed by one or more unauthorized parties."[52] Unlike in *Clapper* where the plaintiffs did not allege that any of their communications had actually been intercepted, the *Chambliss* court established that the data breach *had* occurred and *did* compromise the personal information of CareFirst customers.[53] As the other data privacy cases demonstrate, once a hacker gains access to personal data, there is no need to speculate whether or when identity theft will occur: The only remaining step is for Plaintiffs' information to be misused.[54]

Finally, the *Chambliss* court's narrow interpretation of the injury-in-fact requirement of Article III standing places data breach victims in a difficult situation: They face an increased risk of identity theft, yet they have no legal recourse. The court's conclusion leaves data breach victims waiting until their information is wrongfully used before they can take action to protect themselves. This is problematic because once personal information is compromised in a data breach, the information is readily accessible to the hacker—the only remaining question is not if the information will be used, but when.[55] Further, as the court in *Adobe* recognized, the longer plaintiffs wait for identity theft to materialize, "the more latitude a defendant has to argue that the identity theft is not 'fairly traceable' to the defendant's data breach," creating a separate "standing problem of its own."[56]

A better understanding of technology today should dissuade courts from overly strict interpretations of the injury-in-fact requirement in data privacy cases. Victims of a data beach often look to the courts for relief;[57] the *Chambliss* plaintiffs did just that and found none. The court's holding stands to impede future consumers from holding accountable those who house their most vital information based on a faulty interpretation of standing jurisprudence. A more reasonable approach in an increasingly automated world would afford data breach victims a better opportunity

sqlmap-0150688 (presenting tutorials on how to hack databases and extract "VERY valuable information," which includes names, home addresses, and e-mail addresses) (alteration in original).

52. Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012).

53. *Chambliss*, 189 F. Supp. 3d at 567.

54. *See* Vorbrodt, *supra* note 24, at 109 ("Once this data is accessed and seen by unauthorized eyes, the damage is done—the hackers have all the information necessary to harm the plaintiffs."); *cf. In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (distinguishing *Clapper*'s "chain of assumptions" and stating, "[u]nlike in *Clapper*, where respondents' claim that they would suffer future harm rested on a chain of events that was both 'highly attenuated' and 'highly speculative,' the risk that [p]laintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real").

55. Vorbrodt, *supra* note 24, at 70.

56. *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d at 1215 n.5; *see also supra* note 15 and accompanying text (noting that the alleged future injury must also be fairly traceable to the defendant to satisfy standing).

57. *See* Sid Khaitan, *A Deeper Look into Class-Action Data Breach Lawsuits*, Rippleshot Blog (July 29, 2016, 1:02 AM), http://info.rippleshot.com/blog/a-deeper-look-into-class-action-data-breach-lawsuits (stating that consumer class actions after the announcement of a data breach are a "dime a dozen").

to protect and defend their identities. The court failed to distinguish between the "certainly impending" and "substantial risk" tests, to limit *Clapper* to its unusual facts, and to appreciate the plight of data breach victims. *Chambliss* has set a precedent that leaves victims with no other option but to sit and wait for their stolen information to be used to their detriment.