First Steps in Data Privacy Cases: Article III Standing

Lee J. Plave and John W. Edson

Mr. Plave

Mr. Edson

A recent string of prominent cybersecurity attacks, which have affected parties ranging from Fortune 500 companies to the Democratic National Committee, illuminate the perils of operating a business in an era of ubiquitous connectivity.[1] In September 2017, Equifax Inc., a consumer credit reporting agency, announced that the personal data of nearly 143 million of its users had been compromised by hackers who were able to roam its network undetected for upwards of four months.[2] The fallout from the Equifax data breach has already led to numerous class action lawsuits,[3] the ouster of Equifax's longtime CEO,[4] and a series of very public reprimands on Capitol Hill.[5] In February 2018, the company reportedly confirmed that the extent of the records and details accessed in the hack may be substantially greater—and more troublesome—than initially believed.[6]

1. *See generally* Rachel Abrams, *Target to pay $18.5 Million to 47 States in Security Breach Settlement*, N.Y. TIMES (May 23, 2007), https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html; Ellen Nakashima, *National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns*, WASH. POST (May 18, 2016), https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18.

2. AnnaMaria Andriotis & Robert McMillan, *Hackers Entered Equifax Systems in March*, WALL ST. J. (Sept. 20, 2017), https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617.

3. *See* Eduard Goodman, *The Equifax Data Breach and Its Impact on Business*, LAW360 (Sept. 14, 2017), https://www.law360.com/articles/963870/the-equifax-data-breach-and-its-impact-on-businesses.

4. *See* Ron Lieber & Stacy Cowley, *Replacing Its C.E.O., Equifax Tries To Turn Page*, N.Y. TIMES, Sept. 27, 2017, at B1, *available at* https://www.nytimes.com/2017/09/26/business/equifax-ceo.html.

5. *See* Hamza Shaban, *'This is a Travesty': Lawmakers Grill Former Equifax Chief Executive on Breach Response*, WASH. POST (Oct. 3, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/what-to-expect-from-equifaxs-back-to-back-hearings-on-capitol-hill-this-week.

6. AnnaMaria Andriotis, *Equifax Hack Might Be Worse Than You Think*, WALL ST. J. (Feb. 9, 2018), https://www.wsj.com/articles/equifax-hack-might-be-worse-than-you-think-1518191370

Lee J. Plave (lplave@plavekoch.com) is a partner and John W. Edson (jedson@plavekoch.com) is an associate with Plave Koch PLC in Reston, Virginia.

In October 2017, Yahoo! announced that a 2013 cyberattack, which the company had originally estimated as affecting one billion of its users' accounts, had in fact affected all three billion of its users.[7] In the wake of this breach, Yahoo! stands likely to defend one or more of the largest class action lawsuits in history.[8]

Although the sheer magnitude of the Equifax and Yahoo! data breaches have led these events to dominate headlines, they are only two instances among a proverbial tidal wave of cybersecurity incidents.[9] The Identity Theft Resource Center, a non-profit group that tracks data breaches, estimates that the total number of U.S. data breaches reached an all-time high of 1,579 in 2017, a 45% increase from 2016, and a 102% jump from 2015.[10] The franchise industry is certainly not immune. Wendy's, Jimmy John's, Wyndham Hotels and Resorts, and Sonic Drive-In are among a long list of franchise systems targeted by cyberattacks in recent years.[11]

Although companies that fall victim to a data breach are likely to face a variety of economic and legal consequences,[12] finding an effective way to defend against consumer-driven class action lawsuits stemming from a breach presents one of the most difficult, and potentially costly, challenges.[13] Judi-

(Addressing the breadth and implications of the Equifax breach, the author observed that "[t]he fact that hackers accessed even more data [from Equifax than first reported] shows both the vast amount of information that Equifax holds *and the risks at stake for consumers given the level of personal information that has been compromised*.") (emphasis added).

7. Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES, Oct. 4, 2017, at B2, *available at* https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

8. *See* Taylor Armerding, *Yahoo! Braces Itself for Enormous Class-Action Suit over Breaches*, NAKED SECURITY (Sept. 5, 2017), https://nakedsecurity.sophos.com/2017/09/05/yahoo-braces-itself-as-judge-rules-that-its-on-the-hook-for-a-class-action-suit.

9. *See Data Breaches*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/Data-Breaches/data-breaches (last visited Feb. 13, 2018).

10. *Id.*

11. *See* Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KREBS ON SECURITY (July 8, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/; Brian Krebs, *Jimmy John's Confirms Breach at 216 Stores*, KREBS ON SECURITY (Sept. 24, 2014), https://krebsonsecurity.com/2014/09/jimmy-johns-confirms-breach-at-216-stores/; Craig Timberg, *FTC Sues Wyndham Hotels over Hacker Breaches*, WASH. POST (June 26, 2012), https://www.washingtonpost.com/business/economy/2012/06/26/gJQATDUB5V_story.html; Brian Krebs, *Breach at Sonic Drive-In May Have Impacted Millions of Credit, Debit Cards*, KREBS ON SECURITY (Sept. 26, 2017), https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards.

12. *See generally* Michael K. Lindsey & Mark S. Melodia, *Data Protection and Privacy in Franchising: Who is Responsible?* ABA 36th FORUM ON FRANCHISING, W-16 (2013) (providing an overview of the various economic and legal consequences facing franchise companies that fall victim to a breach).

13. *See* Travis LeBlanc & Jon R. Knight, *A Wake-Up Call: Data Breach Standing is Getting Easier*, CYBER SECURITY LAW REP. (Jan. 17, 2018), at 4, *available at* https://www.bsfllp.com/images/content/2/9/v2/2995/2018-01-17-Cyber-Security-Wake-Up-Call-Data-Breach-Standing-Is.pdf ("In less than two months after its market-moving breach was announced, Equifax incurred $87.5 million in expenses relating to the breach litigation and government investigations."). Obviously, there is also the risk of an enforcement action by a government agency, such as the Federal Trade Commission, which brought such an action against the franchisor of the "Wyndham Hotel" system in 2012. Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 2:13-CV-

cial uncertainty on how to approach these cases has added an extra layer of complexity for companies hoping to develop an effective post-breach litigation strategy.

As private lawsuits stemming from data breaches wend their way through the judicial system, federal courts have struggled to reach a clear consensus on when the owners of compromised data may seek recovery. Specifically, following the Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins (Spokeo I)*,[14] federal courts are split on whether the threat of future harm attributable to a data breach gives a plaintiff standing to sue the company that allegedly failed to protect his or her personally identifiable information (PII).

This article first addresses why recent judicial developments relating to standing in data privacy cases should be of particular importance to franchise companies. Then, the article provides a general overview of the standing doctrine and summarizes recent federal court holdings addressing data privacy standing.

I. Background

Why should franchise companies, in particular, care about tracking federal jurisprudence on a rather technical issue of constitutional law? First, in certain instances, franchise companies have proven to be susceptible to cyberattacks. Second, the likelihood and frequency at which data breach lawsuits make it past the pleading stage would significantly impact a company's data protection policies and litigation strategies. In practical terms, most data breach cases involving franchise systems are either decided in the early stages—for example, a Motion to Dismiss on the issue of standing—or settled. Thus, standing issues have a significant impact on whether a class action brought against a franchisor and its franchisees is dismissed at an early stage or whether the case proceeds ahead (e.g., if standing is found); and if so, the matter is typically resolved by settlement before a trial on the merits.

Unfortunately, some franchise systems have become an attractive target for cybercriminals due to the nature and volume of the information they collect, as well as their inherently diffuse structure.[15] Franchise systems, particularly those in the hospitality and restaurant industries, often have numerous locations, each of which may process hundreds of small credit card transactions a day through an interconnected point-of-sale (POS) system.[16] This

01887-ES-JAD (D.N.J. June 26, 2012). The risk and management of government enforcement actions falls outside the scope of this article.

14. 136 S. Ct. 1540, 1547 (2016), *as revised* (May 24, 2016).

15. *See* Beth Ewen, *Data Breaches Likely Coming to a Franchise Near You, Attorneys Warn*, Franchise Times (May 14, 2015), http://www.franchisetimes.com/news/May-2015/Data-Breaches-Likely-Coming-to-a-Franchise-Near-You-Attorneys-Warn; Tru Pham, *Franchise Data Beaches: Risking the Brand for Franchisee Autonomy*, Duo (Sept. 4, 2014), https://duo.com/blog/franchise-data-breaches-risking-the-brand-for-franchisee-autonomy.

16. *The Impact of Data Breaches on Franchises: Brand Name and Reputational Risk*, Bluefin (Mar. 9, 2017), https://www.bluefin.com/bluefin-news/data-breaches-franchise-name.

steady stream of connected transactions may prove to be a compelling target for resourceful hackers.[17] Complicating matters is that a franchise system is made up of a multitude of independently owned and operated entities utilizing a common brand. Each franchisor and each franchise owner may have a different understanding of its cybersecurity exposure and may have different data protection safeguards and systems. Thus, auditing and implementing system-wide policies may be challenging.

The well-publicized data breach involving the Wendy's restaurant chain highlights the vulnerabilities and consequences that many franchise systems face.[18] In the Wendy's breach, hackers installed malicious software, or malware, on the POS systems that were in use at numerous franchised Wendy's locations.[19] The malware allegedly allowed hackers to collect payment card data (e.g., credit and debit card information, expiration dates, card verification numerals, and PIN data for debit cards) from each customer transaction at the nearly 1,025 Wendy's locations using that POS system.[20]

Once the breach was discovered, Wendy's conducted an internal investigation and determined that a third-party vendor was to blame.[21] Wendy's alleged that hackers somehow acquired the credentials of one of the vendor's employees and used those credentials to access the POS system and install the malware.[22]

Customers affected by the breach argued that Wendy's maintained "an insufficient and inadequate system to protect its customers' private information."[23] These allegations eventually culminated in the filing of two groups of class action lawsuits, one originating from the consumers claiming to have been affected and the other from the financial institutions responsible for reimbursing the resulting fraudulent charges.[24] In the consumer case, the plaintiffs argued, among other things, that the compromise of their personal information put them at a greater risk of future fraud or harm.[25]

The likelihood that consumer lawsuits like the one stemming from the Wendy's breach will make it past the pleading stage has major implications for companies. Perhaps most significantly, the cost of actually litigating, or even settling, a major data breach lawsuit can be astronomical.[26]

17. *Id.*
18. *See* Torres v. Wendy's Co., 195 F. Supp. 3d 1278 (M.D. Fla. 2016); Krebs, *supra* note 11.
19. *Torres*, 195 F. Supp. 3d at 1280.
20. *See id.*; Krebs, *supra* note 11.
21. *Torres*, 195 F. Supp. 3d at 1280.
22. *Id.*; *see also* Verizon, *2017 Data Breach Investigations Report (10th Ed.)* (2017), *available at* https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf (discussing how many data breaches are ultimately attributable to social engineering).
23. *Torres*, 195 F. Supp. 3d at 1281.
24. *See* Jimmy H. Koo, *Wendy's Must Face Credit Card Breach Bank Class Suit*, BLOOMBERG LAW: PRIVACY & DATA SECURITY (Apr. 3, 2017), https://www.bna.com/wendys-face-credit-n57982086138/; *see also Torres*, 195 F. Supp. 3d at 1280.
25. *Torres*, 195 F. Supp. 3d at 1283.
26. *See* Lindsey, *supra* note 12, at 16–17 (discussing data privacy class actions that have resulted in settlement); LeBlanc, *supra* note 13.

Private lawsuits are not the only consequence facing companies that fall victim to a data breach. A breached company will also likely be faced with mitigating damage to its brand reputation,[27] navigating a multitude of breach notification laws,[28] and defending against state and federal law enforcement actions.[29] Thus, with all these competing concerns, the need for some semblance of predictability when crafting a post-breach litigation strategy is abundantly clear.

II. Overview of Standing in Data Privacy Cases Pre-*Spokeo I*

In many data breach lawsuits, plaintiffs who have had their personal data compromised are unable to prove that they are actually the victim of fraud or have suffered any tangible economic loss. Instead, these plaintiffs generally argue that, because of the data beach, they are at a greater risk of future identity theft or other harm.

Historically, federal lawsuits based on the threat of future harm have been easily dismissed at the pleading stage for lack of standing. However, recent federal jurisprudence has signaled a willingness by some circuits to lower the bar necessary for plaintiffs to establish the standing required to bring a case on these grounds.

This section will first provide an overview of the general requirements for establishing Article III standing in federal courts. Next, this section will summarize recent federal court opinions addressing standing in data privacy cases.

A. *General Requirements for Article III Standing*

Article III of the United States Constitution limits the jurisdiction of federal courts to hearing "cases" and "controversies."[30] This limitation is designed to ensure that federal courts remain in their "judicial role" and do not "intrude upon the powers given to the other branches."[31] The doctrine of standing is "rooted in the traditional understanding" of "case" and "controversy" and exists to ensure that the proper litigant is the party bringing a particular lawsuit.[32]

In *Lujan v. Defenders of Wildlife*, the U.S. Supreme Court laid out the "irreducible constitutional minimum" requirements for establishing Article III

27. *See* Ponemon Institute, *The Impact of Data Breaches on Reputation & Share Value* (May 2017), at 3, *available at* https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf.

28. *See* Stephen Embry, *State Data Breach Notification Laws Just Got Crazier*, A.B.A TECH. TRANSLATORS, https://www.americanbar.org/publications/youraba/2016/may-2016/state-data-breach-notification-laws-just-got-crazier.html (last visited Feb. 14, 2018).

29. *See* Abrams, *supra* note 1; Cecilia Kang, *Uber Agrees to Privacy Audits in Settlement with F.T.C.*, N.Y. TIMES (Aug. 15, 2017), https://www.nytimes.com/2017/08/15/technology/uber-agrees-to-privacy-audits-in-settlement-with-ftc.html.

30. U.S. CONST. art. III, § 2, cl. 1; *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), *as revised* (May 24, 2016) (*Spokeo I*).

31. *Spokeo I*, 136 S. Ct. at 1547.

32. *Id.*

standing.[33] Under the *Lujan* test, a plaintiff must show it has: (1) suffered an "injury-in-fact;" (2) that is fairly traceable to the challenged conduct of the defendant; and (3) that is likely to be redressed by a favorable judicial decision.[34] The *Lujan* test requires that the injury-in-fact alleged by the plaintiff must be both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[35]

In data breach cases, the injury-in-fact element has proved to be a difficult hurdle for many plaintiffs to clear because courts are split on whether the inchoate risk of future identity theft or other harm often attributed to a breach is sufficiently concrete to qualify as an injury-in-fact.

B. *Early Circuit Split on Standing in Data Privacy Cases*

Federal courts have reached different conclusions about standing in data privacy cases in recent years. The split in the circuits dates back more than a decade. In a 2007 decision, *Pisciotta v. Old National Bancorp*, the Seventh Circuit advanced a brief, but expansive, interpretation of the injury-in-fact requirement.[36] *Pisciotta* involved a "sophisticated, intentional, and malicious" security breach of a bank's website.[37] Hackers were able to access sensitive information belonging to Old National Bancorp's (ONB) customers and potential customers, which included names, addresses, Social Security numbers, credit card numbers, and other financial account numbers.[38] After learning of the breach, ONB customers filed negligence and breach of contract claims against the bank and its web-hosting provider, NCR.[39]

Interestingly, the plaintiffs did not allege "any completed direct financial loss," nor did they claim that they "already had been the victim of identity theft as a result of the breach."[40] Instead, the plaintiffs argued they were harmed by having to purchase "past and future credit monitoring services" that they had obtained "in response to the compromise of their personal data through ONB's website."[41]

The Seventh Circuit acknowledged the prevailing view in other circuits that plaintiffs whose data had been compromised, but not yet misused, had not suffered an injury-in-fact sufficient to confer Article III standing.[42] Nonetheless, the court held that the injury-in-fact requirement needed to create standing may be established by "a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm

33. 504 U.S. 555, 560–61 (1992).
34. *Id.*
35. *Id.* at 560.
36. 499 F.3d 629 (7th Cir. 2007).
37. *Id.* at 632.
38. *Id.* at 631.
39. *Id.* at 632.
40. *Id.* (emphasis in original).
41. *Id.* at 631.
42. *Id.* at 634.

that the plaintiff would have otherwise faced, absent the defendant's actions."[43]

In *Krottner v. Starbucks Corp*., the Ninth Circuit also showed a willingness to allow plaintiffs to use the threat of future harm to establish standing.[44] *Krottner* involved a stolen Starbucks Corporation laptop containing the unencrypted names, addresses, and Social Security numbers of approximately 97,000 Starbucks employees.[45] When Starbucks learned of the theft, it sent a letter to its employees stating that although there was no indication the private information was misused, the company would nonetheless offer employees free credit reporting services for a limited period of time.[46]

Following receipt of the letter, three Starbucks employees filed suit, alleging negligence and breach of contract.[47] One of the plaintiffs, Krottner, alleged she was spending a "substantial amount of time" reviewing her financial accounts and felt compelled to continue paying for credit monitoring services once the free service expired.[48] Another plaintiff, Lalli, alleged he had developed "generalized anxiety and stress regarding the situation."[49] A third plaintiff, Shamasa, alleged his bank notified him that someone had attempted to open a new account using his Social Security number, although the bank had closed the account before he suffered any financial loss.[50] The district court dismissed the case, finding that the plaintiffs had failed to allege a cognizable injury.[51]

On appeal, the Ninth Circuit reversed, finding that all three plaintiffs had sufficiently alleged an injury-in-fact for purposes of Article III standing.[52] The court held that Lalli easily established standing because he had established a "present injury."[53] However, the appeals court took a more nuanced approach to the allegations of increased risk of future identify theft advanced by Krottner and Shamasa.[54] Acknowledging that it had not yet determined whether the increased risk of identity theft constituted an injury-in-fact, the Ninth Circuit analogized the plaintiffs' allegations to claims of future harm advanced in toxic tort and environmental cases.[55] The court noted that in those contexts it had held that a plaintiff could establish standing as long as the plaintiff faced "a credible threat of harm."[56] Reviewing the

43. *Id.*
44. 628 F.3d 1139 (9th Cir. 2010).
45. *Id.* at 1140.
46. *Id.* at 1140–41.
47. *Id.* at 1141.
48. *Id.*
49. *Id.*
50. *Id.*
51. Krottner v. Starbucks Corp., No. C09-0216-RAJ, 2009 WL 7382290, at *6 (W.D. Wash. Aug. 14, 2009).
52. *Krottner*, 628 F.3d at 1142.
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*

facts in this case, the Ninth Circuit found that the theft of the laptop containing the plaintiffs' PII created a "credible threat of harm" for the plaintiffs that was "both real and immediate, not conjectural or hypothetical."[57]

In *Riley v. Ceridian Corp.*, the Third Circuit rejected the line of reasoning advanced by the Seventh and Ninth Circuits, holding that allegations of "hypothetical, future injury" are not sufficient to establish standing.[58] The dispute in *Riley* arose from the breach of Ceridian Corporation, a payroll processing firm, which allowed a hacker to gain unauthorized access to information about approximately 27,000 employees at 1,900 companies.[59] However, although it was clear that the hacker had accessed Ceridian's database, it was not apparent whether the hacker "read, copied, or understood" the data.[60]

Following the breach, the employees of one of Ceridian's customers filed suit, alleging Ceridian's failure to protect against the breach caused the plaintiffs to (1) suffer an increased risk of identity theft, (2) incur costs to monitor their credit activity, and (3) suffer from emotional distress.[61] In finding that the plaintiffs lacked standing to bring the case, the Third Circuit focused on the speculative nature of the plaintiffs' claims.[62] The court noted that whether the plaintiffs actually suffered any harm relied on the "speculative, future actions of an unnamed-known party," or more specifically, that the hacker had actually "(1) read, copied, and understood their personal information; (2) intended to commit future criminal acts by misusing the information; and (3) was able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [plaintiffs'] names."[63] Since both the skill and the intent of the hacker were unknown, the court held that the threatened harm was neither the "imminent" nor "certainly impending" enough to create the type of injury necessary to establish standing.[64]

C. *Supreme Court's First Opportunity to Provide Clarity*

The U.S. Supreme Court had its first opportunity to clarify Article III standing in data privacy cases in 2013 in *Clapper v. Amnesty International USA*.[65] In *Clapper*, a group of plaintiffs—which included attorneys, journalists, and human rights organizations—challenged the constitutionality of a provision of the Foreign Intelligence Surveillance Act (FISA).[66] The provision in question allowed the U.S. government to conduct surveillance on non-U.S. citizens outside the United States.[67] The plaintiffs, who for a vari-

57. *Id.*
58. 664 F.3d 38, 41 (3d Cir. 2011).
59. *Id.* at 40.
60. *Id.*
61. *Id.*
62. *Id.* at 41.
63. *Id.* at 42.
64. *Id.* at 44.
65. 568 U.S. 398 (2013).
66. *Id.* at 406.
67. *Id.* at 401.

ety of reasons believed they might come into contact with targeted individuals through their work, alleged that their communications would also be captured by government agents.[68] The plaintiffs sought a declaration that the FISA provision was unconstitutional as a violation of their Fourth Amendment rights.[69] The district court dismissed the case for lack of standing, and the Second Circuit reversed on appeal.[70] The Supreme Court ultimately reversed and remanded to the Second Circuit, holding that the plaintiffs lacked standing to assert those claims.[71]

The plaintiffs' argument that they had suffered an injury-in-fact, and therefore had standing to bring the case, was based on two alternative theories.[72] First, the plaintiffs argued there was an "objectively reasonable likelihood" that their communications would be captured.[73] In the alternative, the plaintiffs argued they suffered harm as a result of the additional steps they needed to take to preserve their confidentiality in light of the new provision.[74]

The Supreme Court rejected both arguments. First, the Court rejected the "objectively reasonable likelihood standard" as "inconsistent with [its] requirement that threatened injury must be certainly impending to constitute injury in fact."[75] The Court reasoned that the plaintiffs' theory of harm was based on a "speculative chain of possibilities" and was therefore not "certainly impending."[76] Highlighting policy concerns, the Court also rejected the plaintiffs' alternative argument.[77] The Court concluded that, by allowing plaintiffs to "manufacture standing" based on "their fears of future harm . . . [that] an enterprising plaintiff would be able to secure a lower standard for [standing] simply by making an expenditure based on a non-paranoid fear."[78]

The *Clapper* Court did, however, decide to qualify its "certainly impending" standard and, in doing so, injected an element of ambiguity.[79] In a footnote, the Court explained that in order to establish the future harm was "certainly impending," plaintiffs did not have to prove they were "literally certain" the stated harm would occur.[80] Rather, the Court stated that, in some circumstances, a plaintiff could establish standing by showing there was "substantial risk" that the foreseen harm would occur.[81] Thus, the *Clapper* decision left the door open for varying interpretations of the standard for

68. *Id.* at 407.
69. *Id.* at 401.
70. *Id.* at 407.
71. *Id.* at 408.
72. *Id.* at 401–02.
73. *Id.* at 401.
74. *Id.* at 402.
75. *Id.* at 410.
76. *Id.* at 414.
77. *Id.* at 416.
78. *Id.*
79. *Id.* at 414 n.4.
80. *Id.*
81. *Id.*

injury-in-fact, and the circuits have continued to reach differing conclusions since *Clapper*.[82]

In 2016, the Supreme Court again had an opportunity to set a clear standard for establishing Article III standing in a data privacy case in *Spokeo I*.[83] *Spokeo I* stemmed from alleged violations of the Fair Credit Report Act (FCRA), which was enacted to ensure that credit reporting agencies followed "reasonable procedures to assure maximum possible accuracy of" certain consumer reports.[84]

The defendant, Spokeo, Inc., operated a "people search engine," which aggregates personal information about individuals from the web for a variety uses, such as the evaluation of prospective employees by employers.[85] The plaintiff discovered that his "Spokeo" profile contained inaccurate information and filed suit, alleging that Spokeo, Inc. failed to comply with the terms of FCRA.[86] The district court dismissed the case for lack of standing and the Ninth Circuit reversed.[87] The Supreme Court reversed and remanded the case, holding that the Ninth Circuit had failed to consider all aspects of the injury-in-fact requirement, namely, whether a "concrete harm" existed.[88]

Although the Supreme Court stopped short of saying whether plaintiffs had standing, it provided some guidance by clarifying that a mere statutory violation, without a showing of concrete harm, is not enough to establish Article III standing.[89] However, the Court qualified that a "concrete harm" does not necessarily mean a "tangible harm" in the traditional sense, and that in some cases Congress was equipped to identify "intangible harms" that could establish injury-in-fact.[90] Specifically, the Court explained that "[t]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact; in such a case, a plaintiff need not allege any *additional* harm beyond the one identified by Congress."[91]

Thus, the Supreme Court in *Spokeo I* did not completely open or close the door. Rather, it remanded the case, indicating that a fact-specific inquiry was needed to determine whether an alleged violation of a statutory procedural

82. *Compare* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 694 (7th Cir. 2015) (injuries associated with protecting oneself against future identity theft might suffice as Article III injuries), *and* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390 (6th Cir. 2016) (finding standing to sue on the risk of future harm), *with* Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (allegations of an enhanced risk of future identity theft were too speculative to establish standing).

83. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), *as revised* (May 24, 2016).

84. *Id.* at 1545.

85. *Id.* at 1544.

86. *Id.*

87. *Id.*

88. *Id.* at 1545.

89. *Id.* at 1549.

90. *Id.* at 1543.

91. *Id.* (citing Federal Election Comm'n v. Akins, 524 U.S. 11, 20–25 (1998)) (emphasis in original).

right is—of its own accord—enough to show the "concrete harm" needed to confer standing.[92]

On remand (*Spokeo II*), the Ninth Circuit interpreted *Spokeo I* as confirming that mere procedural statutory violations, absent any other harm, are in some instances sufficient to confer Article III standing.[93] In determining whether a violation of the FCRA could result in the type of concrete injury necessary to establish standing, the court considered: (1) whether the statutory provision at issue was enacted to protect a concrete interest (as opposed to a procedural one); and (2) whether the procedural violation either harmed, or presented a risk of material harm, to that interest.[94] Concluding that a concrete injury existed, the Ninth Circuit reasoned that Congress had enacted the FCRA to "protect consumer privacy," and that the harms resulting from a FCRA violation, namely, material inaccuracies in a consumer report, seemed "patent on their face."[95]

III. Summary of Data Privacy Standing Cases Following *Spokeo I*

Following the Supreme Court's decision in *Spokeo I*, courts in most of the circuits have weighed in on the topic of data privacy standing. More courts seem willing to advance a relaxed interpretation of the injury-in-fact element necessary to establish standing, causing different courts to reach different results on similar facts.

This section summarizes recent holdings involving standing in data privacy cases. The cases are best reviewed in two distinct sub-categories: (1) cases involving alleged statutory violations; and (2) cases resulting from data breaches.

A. *Cases Involving Alleged Statutory Violations*

One line of reasoning adopted in the Third and Eleventh Circuits, as well as other district courts, concludes that, in certain instances, procedural violations of a statute are sufficient to create the injury-in-fact necessary for a plaintiff to establish standing. In contrast, courts in the Second, Seventh, Eighth, and D.C. Circuits have held that, even where Congress has accorded procedural rights to citizens to protect a concrete interest, a plaintiff will not establish standing if the alleged statutory violation presents no material risk of harm to that interest.

1. Third and Eleventh Circuits View: Standing Found

In *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, the Third Circuit held that a procedural violation of the FCRA was, on its own, suffi-

92. *See id.*

93. *See* Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), *cert. denied*, No. 17-806, 2018 WL 491554 (Mem) (U.S. Jan. 22, 2018).

94. *Id.* at 1113.

95. *Id.* at 1114.

cient to establish standing for the plaintiffs.[96] *Horizon Healthcare Services* resulted from the theft of two laptops containing "differing amounts of member information" from Horizon Healthcare Services, Inc.'s headquarters.[97] Shortly after learning of the break-in, Horizon notified its members that their personal information may have been compromised and offered free credit monitoring services.[98]

Four Horizon members subsequently filed suit.[99] In their complaint, the plaintiffs did not allege their identities were stolen as a result of the breach.[100] Instead, they argued Horizon had violated the FCRA by "furnish[ing]" their information in an unauthorized fashion by allowing that information to fall into the hands of thieves and by failing to adopt reasonable procedures to keep the information confidential.[101]

The district court dismissed the case, holding that the plaintiffs did not have standing because they had not suffered a "cognizable injury."[102] The Third Circuit reversed, holding that, in certain instances, a facial violation of a statute was enough to form the injury-in-fact necessary to establish standing.[103] The court reasoned:

> The actual or threatened injury required by Art[icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing, even absent evidence of actual monetary loss. . . . [W]ith the passage of the FCRA, Congress established that the unauthorized dissemination of [plaintiffs'] private information by a credit reporting agency causes an injury in and of itself—whether or not the disclosure of that information increased the risk of identity theft or some future harm.[104]

The court concluded that *Spokeo I* did not modify the injury-in-fact requirement or "erect any new barrier" for plaintiffs hoping to establish standing.[105]

96. 846 F.3d 625, 641 (3d Cir. 2017).

97. *Id.* at 630.

98. *Id.* Offering customers free credit monitoring services is a commonly employed practice for companies that have fallen victim of breach. However, some plaintiffs and courts have viewed offering these services as an admission that the plaintiff is at a greater risk of future harm. *See* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("There is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals. Indeed, Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year").

99. *In re Horizon Healthcare*, 846 F.3d at 631.

100. *Id.*

101. *Id.*

102. *Id.* at 632.

103. *Id.* at 641. Interestingly, in interpreting the Federal Trade Commission Act, the Third Circuit reached a different conclusion in an earlier case involving an alleged data breach at certain Wyndham branded hotels. In *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255–56 (3d Cir. 2015), the Third Circuit applied a cost-benefit analysis to the FTC's argument that possible identity theft, on its own, was enough to establish injury under the FTC Act. The court explained that the relevant inquiry under the FTC Act was whether "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

104. *In re Horizon Healthcare*, 846 F.3d at 639.

105. *Id.* at 638.

To the contrary, the Third Circuit interpreted *Spokeo I* as reemphasizing that Congress "has the power to define injuries" through legislation.[106]

The U.S. District Court for the Northern District of California reached a similar conclusion in *Matera v. Google, Inc.*[107] In *Matera*, the plaintiffs alleged that Google violated various state and federal anti-wiretapping laws through its operation of its "Gmail" application.[108] The plaintiffs alleged that Google intercepted their emails for the dual purposes of (1) providing advertisements targeted to the email's recipient or sender; and (2) creating user profiles to advance Google's profit interests, without the plaintiff's knowledge or consent. Google sought to dismiss the plaintiff's suit for lack of standing.[109]

Citing *Spokeo I*, the district court rejected Google's argument and instead held that, in certain instances, the violation of a right granted by statute may be sufficient to constitute injury-in-fact.[110] However, the court observed in dictum that Google was correct that "not every harm recognized by statute will be sufficiently 'concrete' for standing purposes."[111] The court noted that whether a violation of a statute establishes concrete injury is contingent on two-factors: (1) whether the statutory violation bears a "close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts;" and (2) whether Congress, in enacting the statue, intended for the statutory right to be substantive or procedural.[112]

In applying this test, the *Matera* court first noted that the violation of the wiretapping and privacy laws had a close relationship to the common law tort of invasion of privacy.[113] Second, the court found that Congress had created substantive rights because the statutes were intended to protect individuals from invasions of their privacy.[114]

In 2016, the U.S. District Court for the Southern District of Florida addressed data privacy standing in a case involving a franchise company. In *Flaum v. Doctor's Associates, Inc.*,[115] the court allowed a suit alleging violations of the Fair and Accurate Credit Transaction Act (FACTA) to proceed past the pleading stage, even though the plaintiff had not claimed any present harm.[116]

Flaum involved a consumer class action lawsuit against Doctor's Associates, Inc. (DAI), the franchisor of the Subway sandwich shop system.[117]

106. *Id.*
107. No. 15-CV-04062-LHK, 2016 WL 5339806, at *1 (N.D. Cal. Sept. 23, 2016).
108. *Id.*
109. *Id.*
110. *Id.* at *19; *see also* Van Patten v. Vertical Fitness Group, LLC, 847 F.3d 1037 (9th Cir. 2017) (holding that a facial violation of the Telephone Consumer Protection Act (TCPA) is enough to show a concrete, *de facto* injury because "Congress identified unsolicited contact as a concrete harm, and [by enacting TCPA] gave consumers a means to redress this harm").
111. *Matera*, 2016 WL 5339806, at *9 (emphasis in original).
112. *Id.*
113. *Id.* at *10–11.
114. *Id.* at *10–14.
115. 204 F. Supp. 3d 1337 (S.D. Fla. 2016).
116. *See id.*
117. *Id.*

Flaum alleged that DAI violated FACTA when it printed his full credit card expiration date after he made a purchase at a franchisee-owned Subway shop in Florida.[118] DAI moved to dismiss, arguing that Flaum failed to allege a concrete injury-in-fact and therefore lacked the requisite standing to bring the case.[119]

The district court rejected DAI's motion.[120] Citing *Spokeo I*, the court held that, in certain instances, a statutory violation on its own can create the requisite injury necessary to establish Article III standing, because Congress has the power to elevate to the status of legally cognizable injuries concrete de facto injuries, that were previously inadequate in law."[121] The court explained that the critical inquiry is whether Congress, in enacting FACTA, meant to create "a substantive right for consumers to have their personal credit card information truncated on printed receipts, or merely created a procedural requirement for credit card-using companies to follow."[122]

After analyzing both the nature of the harm the statute was designed to prevent, as well as FACTA's legislative history, the court concluded that Congress had intended to create a substantive privacy right for consumers.[123] Thus, the court concluded that, due to information printed on the receipts, the plaintiffs had suffered "concrete harm," and therefore denied DAI's motion to dismiss for lack of standing.[124]

The Eleventh Circuit adopted a similar approach in two subsequent decisions. In *Church v. Accretive Health, Inc.*, a hospital management company sent the plaintiff a letter advising her that she owed a debt to a particular hospital.[125] The plaintiff filed suit, alleging that the hospital management company had failed to include certain disclosures required by the Fair Debt Collections Practices Act (FDCPA) in the letter.[126]

In *Church*, the plaintiff did not allege that she suffered actual damages from the company's failure to include the FDCPA required disclosures in its letters.[127] Still, the Eleventh Circuit held the plaintiff adequately alleged a concrete injury sufficient to confer standing because: (1) in enacting the FDCPA, Congress created a substantive right to receive the required disclosures in relevant communications; and (2) the defendant violated this substantive right by failing to include the required disclosures in its letter.[128]

Another similar case was heard in the U.S. District Court for the Southern District of Florida. In *Wood v. J Choo USA, Inc.*, the plaintiff, a customer

118. *Id.* at 1338.
119. *Id.* at 1339.
120. *Id.* at 1337.
121. *Id.* at 1340.
122. *Id.* at 1341.
123. *Id.* at 1341–42.
124. *Id.* at 1342.
125. 654 F. App'x 990, 992 (11th Cir. 2016).
126. *Id.*
127. *Id.*
128. *Id.* at 994–95.

of a Jimmy Choo retail store in Palm Beach Gardens, alleged that the retailer violated FACTA after it provided her with a receipt containing her full credit card expiration date.[129] The plaintiff did not allege any tangible harm and instead argued that by violating FACTA, the retailer exposed the plaintiff and the putative class members to an elevated risk of identity theft.[130]

The district court denied the retailer's motion to dismiss for lack of standing, finding that, by enacting FACTA, Congress created a substantive legal right for card-holding consumers to receive receipts truncating their personal credit card numbers and expiration dates and, thus, protecting their personal financial information.[131] According to the court, the plaintiff suffered a concrete harm as soon as the retailer printed the offending receipt, and therefore, had shown the injury-in-fact necessary to establish Article III standing.[132]

2. Second, Seventh, Eighth, and D.C. Circuits: Standing Called into Question

Courts in other circuits have been more reluctant to confer standing to plaintiffs on the mere basis of a statutory violation. In *Strubel v. Comenity Bank*, the Second Circuit determined that an alleged violation of the Truth in Lending Act was not sufficient, on its own, to establish standing if the plaintiff could not show further harm.[133] Rather, the court concluded that:

> [W]e understand *Spokeo*, and the cases cited therein, to instruct that an alleged procedural violation can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents a "risk of real harm" to that concrete interest. But even where Congress has accorded procedural rights to protect a concrete interest, a plaintiff may fail to demonstrate concrete injury where violation of the procedure at issue presents no material risk of harm to that underlying interest.[134]

The Second Circuit has also addressed standing in a case involving alleged FACTA violations.[135] Much like *Flaum* and *Wood*, the plaintiffs in *Cruper-Weinmann v. Paris Baguette America, Inc.* alleged that a retailer violated FACTA when the retailer gave them receipts containing their full credit card expiration date.[136] However, unlike the courts in the Eleventh Circuit, the Second Circuit applied a much narrower interpretation of *Spokeo I*.[137]

129. 201 F. Supp. 3d 1332, 1334 (S.D. Fla. 2016).
130. *Id.*
131. *Id.* at 1340.
132. *Id.*
133. 842 F.3d 181, 185 (2d Cir. 2016).
134. *Id.* at 190.
135. Cruper-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76 (2d Cir. 2017).
136. *Compare Crupar-Weinmann*, 861 F.3d at 77, *with* Flaum v. Doctor's Assocs., Inc., 204 F. Supp. 3d 1337, 1338 (S.D. Fla. 2016) *and* Wood v. J Choo USA, Inc., 201 F. Supp. 3d 1332, 1334 (S.D. Fla. 2016).
137. *Crupar-Weinmann*, 861 F.3d at 77.

Applying *Strubel*, the Second Circuit noted that the key inquiry was whether the retailer's printing of the plaintiff's credit card expiration date on her receipt presented "a material risk of harm to the underlying concrete interest Congress sought to protect in passing FACTA."[138] Concluding that the plaintiff failed to show any material risk of real harm, the court pointed to the fact that Congress itself "*did not* think that the inclusion of a credit card expiration date on a receipt increases the risk of material harm of identity theft." [139]

The Seventh Circuit's 2016 decision in *Meyers v. Nicolet Restaurant of de Pere, LLC* applied an approach that effectively is the same as the Second Circuit's approach in *Cruper-Weinmann.*[140] Similar to other cases alleging FACTA violations, the plaintiff in *Meyers* sued a restaurant that gave him a receipt that failed to truncate his credit card expiration date.[141] The Seventh Circuit in *Meyers* held that the plaintiff had failed to allege concrete injury and, therefore, lacked standing.[142] The court explained that the plaintiff had not suffered a concrete injury because he discovered the violation immediately, nobody else ever saw the receipt, and the mere printing of a card's expiration date, without more, would not heighten the risk of identity theft.[143]

In *Braitberg v. Charter Communications, Inc.*, the Eighth Circuit addressed whether the alleged improper retention of PII, on its own, was sufficient to confer standing.[144] In *Braitberg*, the plaintiff brought a putative class action lawsuit against his former cable television provider, Charter Communications. The plaintiff alleged that Charter violated the Communications Protection Act by retaining personally identifiable information of its customers after they had canceled their subscriptions and after that information was no longer needed to provide services or collect payments.[145] The district court dismissed the case for lack of standing.[146]

The Eighth Circuit upheld the district court, finding that the plaintiff had not shown the concrete harm necessary to establish standing.[147] The Eighth Circuit rejected the plaintiff's argument that, by virtue of a violation of a statutory right, the plaintiff did not need to allege or show any "actual in-

138. *Id.* at 81.

139. *Id.* ("We find it dispositive that in 2007, Congress clarified FACTA in the Credit and Debit Card Receipt Clarification Act of 2007 ("Clarification Act"), stating that '[e]xperts in the field agree that proper truncation of the card number, . . . regardless of the inclusion of the expiration date, prevents a potential fraudster from perpetrating identity theft or credit card fraud.'") (emphasis in original).

140. *Compare* Meyers v. Nicolet Rest. of De Pere, LLC, 843 F.3d 724 (7th Cir. 2016), *with* Cruper-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76 (2d Cir. 2017).

141. *Meyers*, 843 F.3d at 725.

142. *Id.* at 727.

143. *Id.*

144. 836 F.3d 925 (8th Cir. 2016).

145. *Id.* at 927.

146. *Id.*

147. *Id.* at 931.

jury" arising from Charter's retention of his personal information.[148] Citing *Spokeo I*, the court noted that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right," and that Article III "requires a concrete injury even in the context of a statutory violation."[149]

The court found instead that the plaintiff's allegations amounted to "a bare procedural violation, divorced from any concrete harm."[150] The court pointed to the fact that the plaintiff did not allege that Charter had disclosed the information to a third party, that any outside party had accessed the data, or that Charter had used the information in any way during the disputed period.[151]

The D.C. Circuit has also held that statutory violations, absent other harm, did not create the type of injury-in-fact necessary to establish standing.[152] In *Hancock v. Urban Outfitters Inc.*, customers filed suit against Urban Outfitters, Inc. and Anthropologie, Inc., alleging that both retailers violated the District of Columbia Consumer Identification Information Act (CII Act) by requesting customer ZIP codes in connection with consumer credit card purchases.[153] The CII Act states, among other things, that a party may not "request or record the address or telephone number of a credit card holder" as a condition of accepting a credit card as a form of payment for the sale of goods or services.[154] The plaintiffs did not allege any harm beyond being asked for their ZIP codes.[155]

The D.C. Circuit found that the plaintiffs' complaint did "not get out of the starting gate."[156] The court pointed to the fact that the plaintiffs failed to allege any cognizable injury as a result of providing their ZIP codes.[157] Citing *Spokeo I*, the court explained that although a legislature may indeed "'elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law,' the legislature cannot dispense with the constitutional baseline of a concrete injury in fact."[158] Thus, even in claims alleging violation of statutory conferred rights, the asserted injury "must actually exist" and must impact the plaintiff in a "personal and individual way."[159]

148. *Id.* at 930.
149. *Id.*
150. *Id.*
151. *Id.*
152. Hancock v. Urban Outfitters Inc., 830 F.3d 511, 515 (D.C. Cir. 2016).
153. *Id.* at 512.
154. *Id.*
155. *Id.*
156. *Id.* at 514.
157. *Id.*
158. *Id.* (citations omitted).
159. *Id.*

B. *Cases Involving Data Breaches*

In cases involving data breaches, many courts continue to follow the general rule stated in *Clapper*, i.e., that a plaintiff cannot establish standing for "possible future injury" if the threatened injury was not "certainly impending."[160] However, courts in at least four circuits have held that mitigation costs and an increased risk of future harm may, indeed, qualify as cognizable harm sufficient to confer Article III standing.

1. Courts Finding No Standing

In the consumer class action lawsuit resulting from the Wendy's breach referenced in Section I of this article, the U.S. District Court for the Middle District of Florida rejected the notion that the threat of future harm could form the concrete injury necessary to establish standing.[161] In *Torres v. Wendy's Co.*, the plaintiff alleged that shortly after visiting a Wendy's restaurant in Orlando, Florida, his credit union informed him that someone had attempted to use his debit card at a pair of big-box retail stores.[162] The plaintiff informed his credit union that the charges were fraudulent and his account was refunded.[163]

Roughly a month later, the plaintiff learned of the Wendy's breach.[164] Concluding that this was the root of the fraudulent charges, the plaintiff brought a putative class action, alleging that The Wendy's Company had failed to adequately safeguard his and other customers' information against a breach.[165]

The plaintiff did not allege any out-of-pocket loss, but instead claimed, among other things, that by having his information stolen, he faced the "imminent, immediate, and continuing risk of harm from identity theft and identity fraud."[166] The district court dismissed for lack of standing.[167]

In reaching its decision, the district court noted that the plaintiff did not suffer any actual monetary loss as the result of the breach because his credit union refunded the fraudulent charges on his card.[168] The court also held that the threat of future fraud or identity theft was too speculative to create the type of injury necessary to establish standing.[169] Citing *Clapper*, the court noted that for future harm to be sufficient to confer standing, the harm must be "certainly impending."[170] The court held that the future harm alleged in *Torres* did not meet that test because the plaintiff had not reported any ad-

160. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
161. *See* Torres v. Wendy's Co., 195 F. Supp. 3d 1278 (M.D. Fla. 2016).
162. *Id.* at 1280.
163. *Id.* at 1282.
164. *See id.* at 1280.
165. *Id.*
166. *Id.* at 1281.
167. *Id.* at 1285.
168. *Id.* at 1283.
169. *Id.* at 1285.
170. *Id.* at 1283.

ditional fraudulent charges and it was unclear at the time how many other customers were impacted.[171]

The Second Circuit reached a similar conclusion in *Whalen v. Michaels Stores, Inc.*[172] *Whalen* resulted from the 2013 breach of the Michaels Stores, Inc. POS system, which hackers used to access payment card data belonging to Michaels customers.[173] The plaintiff claimed she had used her payment card at a Michaels store around the time of the breach, and based on that fact, brought suit alleging breach of implied contract and violations of New York consumer protection laws.[174]

The plaintiff asserted three alternative theories of injury: (1) that her credit card information was stolen and used twice in attempted fraudulent purchases; (2) that she faced a risk of future identity fraud as a result of the breach; and (3) that she had lost time and money resolving the attempted fraudulent charges and monitoring her credit.[175] The district court dismissed the case for lack of standing.[176]

On appeal, the Second Circuit affirmed, holding that all three of the plaintiff's theories failed to establish the concrete injury necessary to establish Article III standing.[177] First, the court noted that the plaintiff never actually incurred any of the fraudulent charges; instead, these charges were all covered by her card company's fraud insurance policies.[178] Second, the court explained that the plaintiff immediately canceled her payment cards following the breach and that no other personally identifiable information was alleged to be stolen.[179] Finally, the court noted that the plaintiff had failed to plead with specificity the time or effort that she herself has spent monitoring her credit.[180]

2. Courts Holding That the Threat of Future Harm May Establish Standing

In contrast to courts in the Eleventh and Second Circuits, the D.C. Circuit has been more willing to entertain the idea that the threat of future harm is sufficient to establish standing in a case stemming from a data breach. *Attias v. CareFirst, Inc.* related to the 2014 data breach of CareFirst, Inc., which saw a hacker gain access to CareFirst databases containing sensitive customer information.[181] The plaintiffs, CareFirst members, filed a class action suit al-

171. *Id.* at 1284.
172. *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).
173. *Id.*
174. *Id.* at 89–90.
175. *Id.* at 90.
176. *Id.*
177. *Id.* at 90–91.
178. *Id.* at 90.
179. *Id.* at 90.
180. *Id.* at 91.
181. 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, No. 17-641, — U.S. —, 2018 WL 942459 (U.S. Feb. 20, 2018).

leging, among other things, breach of contract, negligence, and violation of various state consumer protection statutes.[182] The district court dismissed the case for lack of standing, finding that the risk of injury to the plaintiffs was "too speculative to establish injury in fact."[183]

On appeal, the D.C. Circuit reversed, holding that that the plaintiffs' alleged risk of injury was "substantial" enough to establish standing.[184] The court noted that it had "frequently upheld claims of standing based on allegations of "substantial risk of future injury" and the proper question to ask at the pleading stage was "whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach?"[185]

Answering this question in the affirmative, the court held that the complaint plausibly alleged that the breach exposed the plaintiffs' sensitive information—notably, their Social Security and credit card information.[186] Based on "experience and common sense," the court noted that plaintiffs would face a substantial risk of identity theft if this sensitive information were accessed by a network intruder.[187]

Finally, the court distinguished *Clapper*, explaining that the fact pattern in *Attias* was not a "series of contingent events" by "independent actions."[188] Instead, the court viewed this situation differently because "an unauthorized party had already accessed personally identifying data on CareFirst's servers" and it was "much less speculative" to "infer that this party has both the intent and the ability to use that data for ill."[189]

The Seventh Circuit has also found the threat of future harm sufficient to establish standing, reasoning that plaintiffs "should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing."[190] *Lewert v. P.F. Chang's China Bistro* stemmed from the 2014 data breach of the P.F. Chang's restaurant chain.[191] As a result of the breach, hackers were able to access the credit and debit card data of many of P.F. Chang's diners.[192] Those customers brought a putative class

182. *Id.* at 623.
183. *Id.* at 622.
184. *Id.* at 629.
185. *Id.* at 627 (emphasis in original).
186. *Id.* at 628.
187. *Id.*
188. *Id.* at 628.
189. *Id.* at 628–29 (citing Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).
190. Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 966 (7th Cir. 2016).
191. *Id.* at 965.
192. *Id.*

action suit against the restaurant chain.[193] The district court dismissed the suit for lack of standing.[194]

The Seventh Circuit reversed, concluding that the plaintiffs had shown the type of sufficiently imminent harm necessary to establish standing under the *Clapper* test.[195] The court explained:

> We identified two future injuries that were sufficiently imminent: the increased risk of fraudulent credit- or debit-card charges, and the increased risk of identity theft. These, we found, were not mere "allegations of possible future injury," but instead were the type of "certainly impending" future harm that the Supreme Court requires to establish standing.[196]

Although courts have shown a differing willingness to find that the threat of future harm can establish standing, each court's analysis does appear to include some fact-driven review of the nature of the breach and the intent of wrongdoer.

C. *Another Trip to the Supreme Court?*

The Supreme Court will surely have many opportunities to provide clarity to the deepening split in the circuits, but it is not clear when or if it will venture into this issue again. The *Spokeo* litigation appeared destined for another trip to the Supreme Court; however in January 2018, the Court denied the petition for certiorari in *Spokeo II*.[197] The Court similarly rejected CareFirst's appeal in *Attias* in February 2018.[198] For the time being, the question of whether standing exists in data privacy cases will be answered on a factual basis, in a case-by-case manner, and will likely be heavily contingent on where the plaintiff files suit.

IV. Conclusion

Developments in technology have created unique opportunities for companies; however, an increased reliance on connectivity entails certain inherent risks. The past decade has seen an alarming jump in data breaches impacting companies, with franchise systems proving to be particularly susceptible.

Judicial uncertainty about how to approach Article III standing in lawsuits resulting from data breaches has added a layer of complexity for companies hoping to establish effective post-breach litigation strategies. In *Clapper* and *Spokeo*, the Supreme Court articulated principles that trial and appellate courts have explored—reaching varying conclusions. While *Clapper* ad-

193. *Id.*
194. *Id.*
195. *Id.*
196. *Id.* at 966.
197. *See* Robins v. Spokeo, Inc., 867 F.3d 1108 (9th Cir. 2017), *cert. denied*, No. 17-806, — U.S. —, 2018 WL 491554 (Mem) (U.S. Jan. 22, 2018).
198. Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, No. 17-641, — U.S. —, 2018 WL 942459 (U.S. Feb. 20, 2018).

dressed harms stemming from an alleged data breaches, and *Spokeo* dealt with claims arising out of statutory violations, we may in the future see cases pled with a variety of claims—for example, a data breach case also involving allegations of statutory breach, which may present even more complex analytic challenges. Although clarity may come from enactment of substantive legislation addressing these issues or from the Supreme Court, franchise companies would be wise to continue monitoring developments and take immediate steps to bolster their comprehensive data protection policies.