Akin®

# Second Circuit Weighs In on Article III Standing in Data Breach Lawsuits, Denying Existence of a Circuit Split

May 19, 2021

Reading Time : **5 min**

By: Natasha G. Kohne

**Background**

To establish standing under Article III, the "plaintiff must have (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."[2] The U.S. Supreme Court has stated that an "injury in fact" requires "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical."[3] Where the injury has not yet occurred, it must be "certainly impending" to constitute an injury in fact; allegations of "possible future injury" or even the "objectively reasonable likelihood" of future injury are insufficient to establish standing.

However, appellate courts have been divided on whether data breach plaintiffs have suffered an injury in fact where their personal information has been improperly accessed or disclosed, but they have not yet experienced identity theft or fraud as a result of the breach. While the Third, Fourth, Eighth and Eleventh Circuits have not recognized the possibility of future harm,[4] the Sixth, Ninth and D.C. Circuits have suggested that the risk of future identity theft could suffice for standing purposes.[5] In *McMorris*, the Second Circuit attempted to reconcile these approaches.

**Procedural History**

In June 2018, an employee of Carlos Lopez & Associates, LLC (CLA), a provider of mental health services to veteran communities, inadvertently sent an email to approximately 65 employees at the company. Attached to the email was a spreadsheet that contained personal information of approximately 130 current and former CLA employees. The data in the spreadsheet included individuals' social security numbers, home addresses, dates of birth, telephone numbers, educational degrees and dates of hire. Three individuals whose information had been shared—Robin Steven, Sean Mungin and Devonne McMorris—filed a class action complaint against CLA and its principal asserting state law claims for negligence, negligence per se, and statutory consumer protection violations on behalf of classes of persons residing in California, Florida, Texas, Maine, New Jersey and New York. The named plaintiffs did not allege that they were victims of fraud or identity theft, that the spreadsheet had been shared with anyone outside of CLA or that their personal information had been misused by third parties. Nevertheless, plaintiffs claimed that they were "at *imminent risk* of suffering identity theft" and becoming victims of "unknown but certainly impending future crimes."[6] Plaintiffs claimed they cancelled their credit cards, purchased credit monitoring and identity theft protection services, and spent time assessing whether to apply for new social security numbers.

Shortly after CLA moved to dismiss the complaint for lack of Article III standing, the parties sought the district court's approval of a class settlement. The district court ordered further briefing on whether plaintiffs possessed Article III standing in advance of the schedule class settlement fairness hearing. On November 22, 2019, the district court denied the motion for approval of the class settlement and instead dismissed the case for lack of subject-matter jurisdiction, noting that the Second Circuit had not yet addressed whether plaintiffs could establish standing based on an increased risk of future identity theft or fraud. The district court also rejected plaintiffs' contention that they suffered injury in fact based on the time and money spent monitoring and changing their financial information and accounts. The court explained, "Plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'"[7] Plaintiff McMorris appealed.

**Risk of Future Identity Theft Can Confer Standing in Some Cases—But Not in *McMorris***

In an opinion written by Judge Sullivan, the Second Circuit held that data breach plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their personal information. After reviewing recent decisions by

other circuits on this issue, the Second Circuit denied the existence of a circuit split and instead commented that "no court of appeals has explicitly foreclosed plaintiffs from establishing standing based on a risk of future identity theft—even those courts that have declined to find standing on the facts of a particular case."[8] The court held that an increased risk of identity theft or fraud **could** be sufficient to establish standing depending on the circumstances. The Second Circuit articulated a nonexhaustive list of factors that its "sister circuits have most consistently addressed" in the data breach context:

> 1. Whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data.
> 2. Whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud.
> 3. Whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[9]

The court emphasized that these factors are "by no means the only ones relevant" to the injury in fact inquiry, and that standing is "an inherently fact-specific inquiry."[10] Applying these factors and finding that the first two weighed in favor of holding that plaintiffs did not establish an injury in fact, the Second Circuit held that plaintiffs failed to plead a sufficient risk of future identity theft or fraud.

The Second Circuit further noted that where plaintiffs take steps to protect themselves following an unauthorized data disclosure, the costs of those proactive measures alone do not constitute an injury in fact. Citing the Supreme Court's guidance in *Clapper v. Amnesty International USA*,[11] the Second Circuit noted that it is only where plaintiffs have shown a substantial risk of future identity theft or fraud that any expenses reasonably incurred to mitigate that risk may qualify as injury in fact.

**Conclusion**

*McMorris* has potentially large implications for data breach victims and companies, not only because it provides the Second Circuit's first definitive guidance on the threshold and oft-litigated issue of standing, but may also impact how federal courts in other circuits approach Article III standing issues related to data breach actions. However, given the nondispositive and nonexhaustive nature of *McMorris*'s three factors, the Second Circuit has left the door

open for parties to assert that other factors should be considered in favor of or against a finding that plaintiffs established an injury in fact sufficient to confer Article III standing.

---

[1] --- F.3d ----, No. 19-4310, 2021 WL 1603808, at *1 (2d Cir. Apr. 26, 2021).

[2] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

[3] *Id*. at 1548 (citation and quotation omitted).

[4] *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44, 45 (3d Cir. 2011); *Beck v. McDonald*, 848 F.3d 262, 274-75 (4th Cir. 2017); *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).

[5] *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027-28 (9th Cir. 2018); *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 59 (D.C. Cir. 2019).

[6] 2021 WL 1603808, at *1 (emphasis added).

[7] *Steven v. Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 807 (S.D.N.Y. 2019) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 416 (2013)).

[8] 2021 WL 1603808, at *3.

[9] 2021 WL 1603808, at *5 (identifying high-risk information as including social security numbers and dates of birth, especially when accompanied by victims' names).

[10] *Id.*

[11] 569 U.S. at 416 (Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

## Categories

Data Breach

Privacy Class Action