Articles + Publications | June 23, 2021

Firmer Footing for Data Breach Standing, Thanks to the Second Circuit

Privacy & Cybersecurity Newsletter

WRITTEN BY

Molly McGinnis Stine | Tara L. Trifon | Matthew Buongiorno

Instead of identifying traditionally "tangible" injuries, data breach plaintiffs typically point to the fact that they *may* be the victim of identity theft at some point in the future. Prior to late April 2021, the federal courts seemed to disagree on whether this mere risk of a future injury after a data breach was sufficient to confer Article III standing. Some circuits (such as the Sixth, Seventh, Ninth, and District of Columbia Circuits) found that such a risk could support standing.[1] Meanwhile, other circuits (such as the Third, Fourth, and Eighth Circuits) reached a different conclusion. A recent Eleventh Circuit decision fell into the middle, embracing an "increased risk plus" analysis. Importantly, though, the Second Circuit in *McMorris v. Carlos Lopez & Associates, LLC*[2] may have resolved any real or perceived circuit split.

The primary issue in *McMorris* was whether the plaintiffs sufficiently articulated an injury to establish standing when their personally identifiable information ("PII") (including Social Security numbers, home addresses, and dates of birth) was inadvertently shared with others at their place of employment. Notably, the plaintiffs did not allege that they were actually victims of fraud or identity theft. Instead, they claimed that they were at "imminent risk" of becoming victims of identity theft or other unknown crimes as a result of the data breach.[3]

The Second Circuit ultimately agreed with the lower court that the mere dissemination of PII—without evidence or allegation that the PII was maliciously targeted or misused—was too speculative to amount to an injury in fact. But the Court formulated a valuable test that will likely aid courts and litigants for the conceivable future.[4]

The Second Circuit's Analysis

To establish standing, a plaintiff must demonstrate that "he or she suffered an injury in fact that is concrete, particularized, and actual or imminent."[5] The Second Circuit acknowledged the Supreme Court precedent that "'allegations of possible future injury' or even an 'objectively reasonable likelihood' of future injury"[6] is insufficient to meet plaintiff's burden.

The court also reinforced the position that "'[a]n allegation of future injury may suffice' . . .'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'"[7] While the court recognized that there is a perception of a circuit split regarding a risk of future identity theft or fraud stemming from a data breach, it noted 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 Second Circuit then endorsed those factors that other courts have considered when finding that the plaintiff did establish standing.

First, it is important to determine whether the third party purposefully obtained plaintiffs' data. Some circuit courts have found that a plaintiff's failure to present evidence or allege that the unauthorized third party *purposefully* obtained plaintiffs' data is too speculative to support Article III standing.[9] On the other hand, courts have found standing when the plaintiff demonstrated that a malicious third party intended to steal data that included plaintiff's information as part of the data breach.[10]

Second, a court is more likely to find standing when there is a showing that some part of the compromised dataset has already been misused. This does not mean that the plaintiff must actually experience any fraudulent activity. Rather, allegations that other customers whose data was compromised in the same data breach suffered misuse are sufficient to satisfy the plaintiff's initial burden. In addition, allegations that the plaintiff's data are being misused can also support a substantial risk of harm sufficient to find standing, even where the misuse has not yet resulted in an actual or attempted identify theft.[11]

Third, courts analyze whether the data at issue are a type that is likely to subject a plaintiff to a perpetual risk of identity theft or fraud after exposure. For example, particularly sensitive, high-risk forms of data like Social Security numbers and dates of birth make it more likely that those victims will be subject to future identity theft or fraud.[12] Less sensitive data—such as publicly available information or data that can be rendered useless to cybercriminals—do not pose the same risks of future injury and are insufficient to confer Article III injury-in-fact.[13]

While the Second Circuit endorsed these factors in determining whether threatened injury was impending, it also acknowledged that these factors are "by no means the only ones relevant to determining whether plaintiffs have shown an injury in fact based on an increased risk of future identity theft or fraud."[14]

Applying these factors to the accidental data disclosure at issue in *McMorris*, the Second Circuit agreed with the district court, finding that plaintiffs failed to plead a meaningful risk of future identity theft or fraud sufficient to establish Article III standing.[15] First, the subject data breach was not part of a sophisticated or malicious cyberattack.[17] Second, the plaintiffs never alleged that their data was in any way misused because of the accidental e-mail.[18] Third, while the subject data included high-risk information, such as Social Security numbers, that alone was insufficient to find an injury in fact, particularly in the absence of any other factor.[19]

Conclusion: Utilizing The Test In Future Cases

It is now settled in the Second Circuit that plaintiffs can establish injury in fact under an increased risk theory – provided the plaintiffs can sufficiently allege facts that meet the three-factor test:

(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 [compromised] dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and
(3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

The effects of this decision will almost certainly extend far beyond the jurisdictional confines of the Second Circuit. Indeed, the Court of Appeals' analysis is perhaps the most comprehensive overview to date of the issue of standing when the plaintiff has merely alleged the risk of future harm to establish an injury in fact. While it remains

to be seen whether courts in other circuits will adopt this test, it can still provide valuable insight as a framework in evaluating the likelihood of data breach claims.

---

[1] *See* Standing on Thin Ice? New Guidance on Standing for Data Breach Claims (March 5, 2021).
[2] *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021).
[3] *Id*.
[4] *See e.g., PEIRAN ZHENG, v. LIVE AUCTIONEERS LLC.*, No. 20-CV-9744 (JGK), 2021 WL 2043562, at *3 (S.D.N.Y. May 21, 2021) (utilizing the test set forth in *McMorris* to find that the plaintiff set forth a prima facie showing of Article III standing because he alleged that the relevant data was taken by a malicious third party and sold to others).
[5] *McMorris*, 995 F.3d at 299-300. In addition, a plaintiff must demonstrate that the injury was caused by the defendant and that the injury would likely be redressed by the requested relief. *See Thole v. U.S. Bank N.A.*, — U.S. –, 140 S.Ct. 1615, 1618, 207 L.Ed.3d 85 (2020).
[6] *McMorris*, 995 F.3d at 300 (citing *Clapper Amnesty Int'l USA*, 568 U.S. 398, 409-10 (2013)).
[7] *Id*. (citing *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)).
[8] *Id*.
[9] *Id*. at 301 (citing *Beck v. McDonald*, 848 F.3d 262, 274-75 (4th Cir. 2017); *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012)).
[10] *Id*. (citing *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)).
[11] *Id*. at 301 (citing *In re Zappos.com, Inc*., 888 F.3d 1020, 1027 n. 7 (9th Cir. 2018), *Fero v. Excellus Health Plan, Inc*., 304 F. Supp. 3d 333, 341, 344–45 (W.D.N.Y. 2018), and *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig*., 928 F.3d 42, 57–58 (D.C. Cir. 2019)).
[12] *Id*. at *5 (citing *Attias v. CareFirst, Inc*., 865 F.3d 620, 628 (D.C. Cir. 2017)).
[13] *Id*. (citing *Whalen v. Michaels Stores, Inc*., 689 F. Appx. 89, 90 (2d Cir. 2017); *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021).
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber