May 4, 2021

Second Circuit Clarifies Standing Inquiry in Data Breach Actions

On April 26, 2021, the Second Circuit Court of Appeals in *McMorris* v. *Carlos Lopez & Associates, LLC*[1] affirmed the dismissal of a putative class action arising from a data breach for lack of Article III standing. In the *McMorris* case, employees of defendant Carlos Lopez & Associates, LLC ("CLA") alleged that their personally identifiable information ("PII") was compromised when another employee accidentally circulated sensitive information via email within the company. The court held that plaintiffs did not adequately establish Article III standing because the compromised data was the subject of inadvertent disclosure, rather than intentionally targeted theft. But in doing so, the court acknowledged that a risk of future harm, and not just proven actual misuse, can provide sufficient injury-in-fact to establish standing in certain circumstances. Defendants in data breach cases may benefit from the distinction the Court drew between inadvertent disclosure and data theft, as well as the Court's rejection of standing based on the time and costs plaintiffs expended seeking to mitigate risks from the breach. Plaintiffs, on the other hand, will likely rely heavily on the Court's explicit recognition that Article III standing may be present where plaintiffs show only a future risk of potential misuse. Depending of course on developments in future cases, the *McMorris* ruling may prove to be an important decision that clarifies the fault lines of Article III standing in data breach cases.

Background

Data privacy lawsuits have presented novel challenges to courts seeking to apply traditional concepts of Article III standing—particularly the requirement that plaintiffs show they have suffered, or will imminently suffer, a cognizable injury. Courts and commentators have identified a split between the decisions of the Courts of Appeals, with some circuits requiring a plaintiff to show that a malicious actor (i.e., a hacker) has obtained *and* misused the plaintiff's data, and other circuits requiring only that the plaintiff show that the circumstances of the data breach give rise to a substantial likelihood of future misuse.[2]

The circumstances of this case speak directly to the fault line in data breach standing cases between cases involving targeted, malicious hacks and misuse and those cases involving inadvertent loss of data. The suit arose when an employee of CLA, a provider of mental health services to veterans, accidently forwarded a

---

1 --- F.3d ---, 2021 WL 1603808 (2d Cir. Apr. 26, 2021).

2 *Compare In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, 888 F. 3d 1020, 27 (9th Cir. 2018) (holding plaintiffs have standing "based on a substantial risk that the . . . hackers" in possession of their PII "will commit identity fraud or identity theft."), *with Reilly* v. *Ceridian Corp.*, 664 F.3d 38, 40, 44 (3d Cir. 2011) (where there "has been no misuse of the information, [there is] no harm.").

spreadsheet containing PII of approximately 130 current and former CLA employees to approximately 65 current CLA employees.[3] The forwarded PII included social security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire.[4] Three CLA employees brought a putative class action in the Southern District of New York alleging various state law tort and consumer protection claims. CLA moved to dismiss.

Before briefing on the motion to dismiss was complete, the parties reached a settlement. Nevertheless, Judge Jesse Furman rejected the settlement at the fairness hearing and dismissed the case, raising *sua sponte* the issue of whether the district court had subject-matter jurisdiction over the claims, and whether plaintiffs had adequately established Article III standing. Judge Furman found that the plaintiffs had failed to establish standing. In his decision, he noted that data breach cases in which courts ordinarily find standing "have a common denominator. In each of them, the plaintiffs' data actually had been [targeted and taken] by one or more unauthorized third parties"—a fact the court found not present in the case at hand.[5]

Moreover, the district court rejected plaintiffs' assertion of cognizable injury resulting from the time and costs expended mitigating potential fallout from the breach, holding this was insufficient for standing purposes because "Plaintiffs cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[6] Plaintiffs appealed to the Second Circuit.

The Second Circuit's Decision

In a unanimous decision authored by Judge Richard Sullivan, the Second Circuit affirmed the district court's rejection of the settlement and dismissal of the case. The court began by endorsing the district court's analysis of the particular factors to be used to evaluate whether a data breach plaintiff has sufficiently alleged Article III standing based on likelihood of future injury.[7] These factors include:

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; and

---

3 *Steven* v. *Carlos & Lopez Associates, LLC*, 422 F. Supp. 3d 801 (S.D.N.Y. 2019).

4 *McMorris*, --- F.3d ---, 2021 WL 1603808, at *1.

5 422 F. Supp. 3d at 805 (citing *Katz* v. *Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012).

6 *Id.* at 807 (internal quotations marks omitted) (citing *Clapper* v. *Amnesty Intern'l*, 568 U.S. 398, 416 (2013)).

7 *McMorris*, --- F.3d ---, 2021 WL 1603808, at *4.

3. Whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[8]

The court clarified that these factors are non-exhaustive, but also emphasized that they appeared to be the salient factors other circuits have considered when evaluating standing in data breach cases.[9] The first factor, whether the data was exposed as a result of a targeted hack, was singled out by the court as the "most important[ ]" determinant in the standing inquiry.[10]

Applying these factors, the court agreed with the lower court that plaintiffs failed to show Article III standing.

- *First*, the court highlighted the fact that "Plaintiffs never alleged that their data was intentionally targeted or obtained by a third party outside of" the organization,[11] emphasizing instead, that plaintiffs alleged only that their PII had been inadvertently disclosed in "an unauthorized manner" to approximately 65 current employees. The court characterized the incident as being far from a sophisticated cyber-attack.[12] As a result, the court held that this first factor did not favor standing.

- *Second*, the court found that "Plaintiffs d[id] not allege that their data (or the data of any other then-current or former . . . employees) was in any way misused because of the accidental email."[13] Accordingly, the court also held that this second factor did not favor standing.

- *Third*, the court acknowledged that the PII at issue in this case was particularly sensitive (particularly social security numbers and dates of birth), but found that the third factor "alone does not establish an injury in fact."[14] The court held that this factor favored standing.

Although the third factor favored standing, the court determined that the plaintiffs had failed to overcome the first two factors to sufficiently allege a cognizable present or likely future injury for Article III standing purposes. The court also affirmed the district court's holding that, where a plaintiff fails to sufficiently allege that they suffered a present or likely future injury, the plaintiff cannot then assert that costs incurred to

---

8 *Id.* at *4–5.

9 *Id.* at *4.

10 *Id.* at *4.

11 *Id.* at *5.

12 *Id.*

13 *Id.* at *6.

14 *Id.*

mitigate the risk of future data misuse are independent grounds for Article III standing.[15] Accordingly, the court held the plaintiffs lacked standing under this theory because they failed to allege a sufficient likelihood of future injury.

Finally, the court declined to address an additional theory of standing that data breach plaintiffs frequently rely on: namely, that they have standing as a result of any violation of their statutory rights, such as those "designed to protect individuals' privacy."[16]

Implications

The Court's decision provides a framework to assess whether plaintiffs have Article III standing in data breach cases. District courts in the Second Circuit and beyond may rely on the decision when determining whether a plaintiff in a data breach case has suffered sufficient injury to confer standing—particularly given the absence of any nationwide guidance from the Supreme Court on standing in data breach cases. The Second Circuit's effort to provide coherence to the standing analysis in such cases will help parties determine the viability of a potential suit and the appropriate point at which to seek a settlement—a particularly important development considering data breach cases are usually settled or dismissed on a dispositive motion—with standing often one of the most frequently litigated issues.

Both defendants and plaintiffs in data breach cases will likely cite to the decision.

- Defendants in cases involving data breaches due to an accident or circumstances other than a clear intentional hack (for instance, where the cause of the breach remains largely undetermined) may benefit from the Court's emphasis on the importance of plaintiffs showing their PII was acquired specifically through a targeted, malicious hack. Additionally, defendants will likely appreciate the Court's rejection of standing based on a plaintiff's mitigation costs in the absence of a sufficient showing of actual or imminent harm. The mitigation theory has thus far been a common and relatively straightforward theory of standing in data breach cases, the viability of which is now sharply limited in the Second Circuit.

- Plaintiffs in data breach cases may take heart that the Second Circuit decision does not always require proof that the particular plaintiff's data has been misused in order to establish standing. Instead, the court made clear that plaintiffs need not show that *their* particular data has been misused in order, but instead can show that they face a sufficient likelihood of future misuse in order to show cognizable injury. Plaintiffs in cases involving intentional hacks but no evidence of misuse may benefit from this decision.

---

15 *Id.* at *5.

16 *Id.* at *3 n.3.

The decision also raises issues that district courts applying the decision will likely need to confront, including:

- How should courts weigh each of the three factors in their analyses? (e.g., is an intentional hack itself sufficient injury even if the other two factors weigh against standing)?
- Under what circumstances can plaintiffs whose PII was exposed through circumstances other than an intentional hack prove they have standing?
- To what extent will district courts find standing based on an alleged violation of a plaintiff's rights under statutes designed to protect individual privacy rights? This is a question the Court expressly declined to address in its decision.

We will continue to monitor developments in this space.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Susanna M. Buergel
+1-212-373-3553
sbuergel@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jane B. O'Brien
+1-202-223-7327
jobrien@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associates Charles P. Sucher and Cole A. Rabinowitz, and Staff Attorney Bertie Cheng, contributed to this memorandum.