SULLIVAN & CROMWELL LLP

S&C memo

April 30, 2021

Second Circuit Clarifies Standard for Article III Standing In Data Breach Actions

Court Adopts Factors to Evaluate Whether an Increased Risk of Future Harm Resulting From a Data Breach Confers Standing

SUMMARY

On April 26, 2021, the United States Court of Appeals for the Second Circuit issued a unanimous opinion in *McMorris* v. *Carlos Lopez & Associates, LLC* [1] affirming the dismissal, on Article III standing grounds, of a class action predicated on the plaintiffs' alleged increased risk of identity theft or fraud arising out of their employer's accidental email dissemination of their sensitive personal information to other employees within the company. The Second Circuit held that, although plaintiffs may in some cases establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data, district courts should consider a number of factors related to the nature of the data and its exposure or misuse in determining whether an increased risk has, in fact, been adequately alleged or established. After considering those factors, the court concluded that the plaintiffs had failed to allege such an increased risk because, among other reasons, they did not allege that the disclosure was intentional or that their data (or the data of any other person whose data was disclosed) had been misused.

BACKGROUND

McMorris bears on what the Second Circuit described as the "intersection" of "data breaches and inadvertent mass emails."[2] In *McMorris*, an employee of Carlos Lopez & Associates, LLP ("CLA") accidentally sent an email to dozens of CLA employees that attached a spreadsheet containing the "personally identifiable information ('PII')—including Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees, and dates of hire—of approximately 130 then-current and former CLA employees."[3] CLA took no corrective action other than to inform the then-current employees

whose PII had been disclosed of the accidental email.[4] Thereafter, three of the individuals whose PII had been exposed ("Plaintiffs") filed a class action complaint against CLA asserting various state law claims.[5] Plaintiffs alleged that CLA's disclosure of Plaintiffs' PII put them "at imminent risk of suffering identity theft" and left them vulnerable to "impending future crimes," in anticipation of which they cancelled their credit cards, purchased identity theft protection services, and assessed their need to apply for new Social Security numbers.[6]

The parties reached a class settlement, which they asked the district court to approve. The district court, however, *sua sponte* raised the question whether Plaintiffs had Article III standing to bring their claims—a threshold, jurisdictional question of which federal courts must always satisfy themselves before adjudicating a case.[7] Specifically, the district court questioned the first element necessary to establish Article III standing, *i.e.*, whether Plaintiffs had suffered an injury in fact "that is concrete and particularized and actual or imminent, not conjectural or hypothetical."[8]

Following a class settlement fairness hearing, the district court denied the motion for approval because it lacked subject-matter jurisdiction.[9] In concluding that Plaintiffs lacked Article III standing, the district court reasoned that (i) the Second Circuit, unlike the First, Third, Fourth, Seventh, Eighth, Ninth, Eleventh, and District of Columbia Circuits, had not concluded that an increased risk of future identity theft or fraud following an inadvertent disclosure of data can establish an injury in fact; (ii) even if it had, Plaintiffs had not alleged that they faced "'certainly impending' identity theft or fraud, or even a 'substantial risk' of such harm" as a result of the disclosure of their PII,[10] as required under *Susan B. Anthony List* v. *Driehaus*;[11] and (iii) Plaintiffs' proactive measures to prevent harm resulting from the disclosure of their PII could not establish an injury in fact as it amounted to, "in essence, inflicting harm on themselves based on a speculative fear of future identity theft."[12]

THE SECOND CIRCUIT'S DECISION

Recognizing that it was a question of first impression in the Second Circuit, the court acknowledged, consistent with every other Circuit to have addressed it, that "plaintiff[s] *may* establish standing based on a risk of future identity theft or fraud stemming from the unauthorized disclosure of [a] plaintiff's data"[13] (*i.e.*, based on a so-called "'increased-risk' theory").[14] The court then held that courts considering whether plaintiffs have adequately alleged an Article III injury-in-fact based on the increased-risk theory "should consider . . . [three] non-exhaustive factors"[15] that "bear on whether the risk of identity theft or fraud is sufficiently 'concrete, particularized and . . . imminent'":[16]

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. Whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.[17]

The court emphasized that, although these factors are merely illustrative, they are the considerations that other Circuits have "most consistently addressed," and "provide helpful guidance in assessing whether plaintiffs have adequately alleged an injury in fact."[18]

In addition, drawing upon Supreme Court precedent noting that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending,"[19] the court also concluded, consistent with the district court, that the cost of proactive measures taken by plaintiffs to protect themselves following an unauthorized data disclosure cannot alone constitute an injury in fact.[20]

Applying the principles it articulated, the Second Circuit easily concluded that "Plaintiffs have failed to show that they are at a substantial risk of future identity theft or fraud sufficient to establish Article III standing."[21] In particular, (1) Plaintiffs had not "alleged that their data was intentionally targeted or obtained by a third party outside of CLA";[22] (2) Plaintiffs had not alleged "that their data (or the data of any other then-current or former CLA employee) was in any way misused because of the accidental email";[23] and (3) although the information that was disclosed by CLA, including Social Security numbers, was "the sort of PII that might put Plaintiffs at a substantial risk of identity theft or fraud . . . this factor alone d[id] not establish an injury in fact."[24]

Accordingly, the Second Circuit affirmed the district court's dismissal of Plaintiffs' complaint for failure to establish an Article III injury in fact, noting that, to hold otherwise, would be permitting Plaintiffs to string together a speculative "chain of possibilities"—*i.e.*, that then-current CLA employees would either misuse the data themselves or expose the spreadsheet containing the data to a malicious third party that would, in turn, misuse Plaintiffs' PII.[25]

Notably, *McMorris* expressly did not address the "separate but related question of whether plaintiffs may allege a *present* injury in fact stemming from the violation of a statute designed to protect individuals' privacy, which primarily involves the application of the Supreme Court's decision in *Spokeo* . . . ."[26] In *Spokeo, Inc.* v. *Robins*,[27] the Supreme Court held that even an "intangible harm" will be sufficient to establish a present injury in fact if it either "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," or is one that Congress has otherwise "elevat[ed] to the status of legally cognizable injuries."[28] Some courts of appeals have since interpreted *Spokeo* to mean that the mere violation of certain statutes that are intended to protect individuals' privacy, such as the Fair Credit Reporting Act or the Fair Debt Collection Practices Act, is sufficient to establish a present injury in fact.[29] The Second Circuit was careful to emphasize that, in *McMorris*, Plaintiffs brought claims asserting only a *future* risk of theft or fraud, so it had "no reason to address this privacy-based theory of standing."[30]

IMPLICATIONS

The *McMorris* decision is significant because it is the first time the Second Circuit has ruled that plaintiffs may potentially have standing to bring data breach litigation based on the risk of future harm arising from the breach of their personal information. At the same time, the decision requires courts to analyze and consider carefully the circumstances under which future risk of harm may be grounds for litigation to proceed. In articulating factors that courts should consider in determining whether the future harm is sufficiently concrete, particularized and imminent to confer standing, the Second Circuit has made clear that courts should not entertain a speculative "chain of possibilities" that harm could ensue as alleged by plaintiffs in an effort to gain standing.

The non-exhaustive factors articulated by the Second Circuit for districts courts to consider should narrow the scope of cases in which a risk of future harm can confer standing. For example, the first factor—whether the data was taken as part of a targeted attempt to obtain the data—will weigh against a finding of standing in the many cases in which PII is inadvertently sent out of the company (as in *McMorris*) or exposed by the company only as a result of misconfiguration in a cloud computing environment that enables access to data by individuals, such as security researchers, who are unlikely to misuse it. Similarly, the considerations as to whether the data has already been misused, and whether it is sensitive, will weigh against a finding of standing in data breach situations in which individuals' personal information has been exposed and notification to those individuals is required under data breach notification laws, but where that information is not misused or particularly sensitive. This may happen, for example, when the exposure is incidental, both in non-criminal breaches and in deliberate cyber attacks in which the perpetrators' goal is to cause other types of harm besides harm to individuals. This may also happen, for example, where the personal information at issue can easily be changed to mitigate the risk of harm, such as with a compromise of customer account numbers.

Ultimately, *McMorris* brings the Second Circuit largely in line with all the other Circuits to have specifically considered this issue, including the First, Third, Fourth, Seventh, Eighth, Ninth, Eleventh, and District of Columbia. Notably, plaintiffs have not had significant success in these other Circuits in demonstrating standing where, as in *McMorris*, the future harm is largely speculative. For instance, in *Beck* v. *McDonald*,[31] the court concluded that plaintiffs lacked Article III standing because they had "uncovered no evidence that the information contained on the [allegedly] stolen laptop[s] ha[d] been accessed or misused or that they ha[d] suffered identity theft."[32] Likewise, in *Tsao* v. *Captiva MVP Restaurant Partners, LLC*,[33] the court concluded that the plaintiff did not have Article III standing following a data breach in which plaintiff alleged "hackers *may* have accessed and stolen customer credit card data" because it was "unlikely that the information allegedly stolen . . . standing alone, raise[d] a substantial risk of identity theft."[34] By contrast, cases in which other Circuits have found Article III standing based on an increased risk of harm have involved, for instance, allegations that a malicious third party intentionally targeted the defendant's system

and stole plaintiffs' data stored on that system[35] or allegations that a data breach of an online retailer's customer database had resulted in fraudulent charges actually being placed on certain customers' credit cards (albeit not on the plaintiffs').[36] Thus, while the *McMorris* decision allows for the possibility that plaintiffs may demonstrate standing based on an increased risk of future harm, the decision directs courts to scrutinize these standing claims closely, and to heed the Second Circuit's guidance that a speculative chain of possible harms alone will fail to confer standing on plaintiffs in data breach litigation.

* * *

ENDNOTES

1 No. 19-4310, 2021 WL 1603808 (2d Cir. Apr. 26, 2021).

2 *Id*. at *1.

3 *Id.*

4 *Id.*

5 *Id.*

6 *Id.* (citation omitted).

7 Fed. R. Civ. P. 12(h)(3).

8 *Steven* v. *Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 804 (S.D.N.Y. 2019) (quoting *Spokeo, Inc.* v. *Robins*, 136 S. Ct. 1540, 1548 (2016)).

9 *McMorris*, 2021 WL 1603808, at *2 (citing *Steven*, 422 F. Supp. 3d at 807).

10 *Id.* (citing *Steven*, 422 F. Supp. 3d at 804).

11 573 U.S. 149, 158 (2014).

12 *McMorris*, 2021 WL 1603808, at *2 (citing *Steven*, 422 F. Supp. 3d at 807).

13 *Id*. at *3 (emphasis added).

14 *Id*. at *4.

15 *Id.* at *5.

16 *Id*. at *4 (alteration in original) (quoting *Thole* v. *U.S. Bank N.A*., 140 S. Ct. 1615, 1618 (2020)).

17 *Id.* at *5.

18 *Id.*

19 *Id.* (quoting *Clapper* v. *Amnesty Int'l USA*, 568 U.S. 398, 416 (2013)).

20 *Id*. at *6.

21 *Id*. at *5.

22 *Id.*

23 *Id.* at *6.

24 *Id*.

25 *Id*.

26 *Id.* at *4 n.3 (alteration in original).

27 136 S. Ct. 1540 (2016).

28 *Id.* (citation and alterations omitted).

29 *See, e.g.*, *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 636–39 (3d Cir. 2017).

30 *McMorris*, 2021 WL 1603808, at *4 n.3.

31 848 F.3d 262 (4th Cir. 2017).

32 *Id.* at 274.

33 986 F.3d 1332 (11th Cir. 2021).

ENDNOTES (CONTINUED)

[34] *Id.* at 1343 (emphasis in original).

[35] *See Remijas* v. *Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

[36] *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1027–28 (9th Cir. 2018).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.