GIBSON DUNN

Second Circuit Seeks to Reconcile Circuit Split Concerning Standing to Bring Data Privacy Lawsuits

Client Alert | April 30, 2021

On April 26, 2021, in *McMorris v. Carlos Lopez & Associates, LLC*,[1] Judges Calabresi, Katzmann, and Sullivan of the Second Circuit entered the muddy waters at the intersection of data privacy and constitutional law in addressing when a plaintiff in a data breach case has suffered a sufficient injury to establish standing to bring a lawsuit in federal court under Article III of the United States Constitution based on an increased risk of future identity theft. This question presented a matter of first impression for the Second Circuit, which sought to harmonize the divergent approaches taken by its sister circuits on this pressing—and oft-recurring—issue by articulating a non-exhaustive three-factor test to aid courts' future adjudication of these highly fact-specific disputes. Applying this test, the Second Circuit affirmed the district court's dismissal for lack of standing because the plaintiffs had failed to plead a sufficient risk of future identity fraud.

I. Article III Standing and Data Privacy

Under Article III of the United States Constitution, "federal courts lack jurisdiction if no named plaintiff has standing."[2] To establish standing, plaintiffs must demonstrate that they have (1) "suffered an injury in fact" (2) that "was caused by the defendant," and which (3) "would likely be redressed by the requested judicial relief."[3] In turn, 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.'"[4] While an alleged risk of future harm may suffice, a mere "possible future injury" or even an "objectively reasonable likelihood" of a future injury is not enough to meet the injury in fact requirement.[5] Instead, the future injury must be "certainly impending" or there must be "a substantial risk that the harm will occur."[6]

Whether an injury in fact has been adequately pleaded is often a threshold issue raised at the motion to dismiss stage in litigation concerning data breaches. Despite the frequency with which this question arises, however, it is widely recognized that "courts have struggled" to answer it in a consistent manner[7] and the federal courts of appeals "are divided."[8]

For instance, the D.C. Circuit has found it "at least plausible" that data breach victims "run a substantial risk of falling victim" to future identity theft, particularly where some plaintiffs "have already experienced some form of identity theft since the breaches."[9] Similarly, the Ninth Circuit suggested that it was sufficient for standing purposes if hackers "accessed information that could be used to help commit identity fraud or identity theft" or had "the means" to access such information going forward in light of the data breach.[10]

On the other hand, the Third Circuit has long held that plaintiffs lack standing if "no misuse is alleged" and there is "no quantifiable risk of damage in the future."[11] More recently, the Eighth Circuit similarly held that "a mere possibility" of future harm following hackers' theft of financial information was not a constitutionally cognizable injury,[12] and earlier this year the Eleventh Circuit agreed that "a mere data breach does not, standing alone,

Related People

Jeremy S. Smith

Michael L. Nadler

satisfy the requirements of Article III standing."[13]

II. Facts and Procedural History of *McMorris*

In June 2018, an employee at Carlos Lopez & Associates, LLP ("CLA") accidentally sent a spreadsheet containing the Social Security numbers, home addresses, dates of birth, telephone numbers, hiring dates, and other personal information for approximately 130 current and former CLA employees to all of the company's then-current employees.[14] Three individuals whose personally identifiable information was disclosed filed a class-action complaint against CLA, asserting various state-law claims and alleging two distinct injuries.[15] First, they claimed that the disclosure put them "'at imminent risk of suffering identity theft' and becoming the victims of 'unknown but certainly impending future crimes.'"[16] Second, they alleged they were injured "in the form of the time and money spent monitoring or changing their financial information and accounts."[17] Notably, however, they never alleged that their personal information was actually shared outside of CLA or misused by anyone.

Although the parties reached a proposed class settlement, Judge Furman of the United States District Court for the Southern District of New York declined to approve the settlement and instead dismissed the matter *sua sponte* for lack of subject-matter jurisdiction.[18] In doing so, he held, that the plaintiffs' alleged increased risk of future identity theft was not sufficiently concrete to support standing.[19] With no allegations that CLA's release of personal information was intentional, involved malicious third parties, or had caused any actual misuse of data, Judge Furman found the plaintiffs' injury too speculative and attenuated to qualify as an injury in fact.[20] He also rejected their theory of injury based on the actual costs they had incurred as a result of the disclosure of their personal information, reasoning that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[21] Since the possibility of identity theft was speculative, any costs taken to avoid it did not qualify as injuries in fact.

III. The Second Circuit's Legal Analysis

In an opinion written by Judge Sullivan, the Second Circuit affirmed the district court's dismissal of the claims against CLA for lack of standing.

While it recognized that other circuits had wrestled with the question of "whether a plaintiff may establish standing based on a risk of future identity theft or fraud stemming from the unauthorized disclosure of that plaintiff's data,"[22] the Second Circuit sought to bridge the apparent divide. Its reading of its sister circuits' decisions was that none had "explicitly foreclosed" a future-harm theory.[23] Instead, Judge Sullivan reasoned that the Third, Eighth, and Eleventh Circuits had only "declined to find standing on the facts of a particular case."[24] The Second Circuit therefore characterized itself as "join[ing] all of [its] sister circuits that have specifically addressed the issue in holding that plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data."[25]

However, the Second Circuit did not hold that *any* such allegation was sufficient to plead an injury in fact. Instead, it endorsed three non-dispositive and non-exhaustive factors that, it said, other appellate courts have "consistently addressed in the context of data breaches and other data exposure incidents" as providing "helpful guidance" in assessing the presence or absence of constitutional standing: "(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."[26]

Applying these factors to CLA's data disclosure, the Second Circuit held that the plaintiffs had failed to plead a sufficient risk of future identity theft or fraud to establish Article III

standing. The first two factors weighed in favor of dismissal in *McMorris* because the case "merely involve[d] the inadvertent disclosure of [personal information] due to an errant email,"[27] not a targeted or malicious attempt to obtain data, and the plaintiffs never alleged that any of "the exposed dataset was compromised."[28] Although the third factor weighed in favor of finding that the court had Article III jurisdiction because the disclosed data "included the sort of [personally identifiable information] that might put Plaintiffs at a substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the [data] was intentionally taken by an unauthorized third party or otherwise misused," the Second Circuit held that "this factor alone does not establish an injury in fact."[29] As such, the first two factors proved fatal to plaintiffs' claimed standing based on a risk of future harm. And, as a result, the plaintiffs' claims based on their protective-measures theory also failed because absent "a substantial risk of future identity theft," any efforts "protecting . . . against [a] speculative threat cannot create an injury.[30]

IV. Conclusion

Whether *McMorris* effectively synthesized the federal judiciary's "disarray about the applicability of [the] 'increased risk' theory in data privacy cases"[31] or only (inadvertently) highlighted the stark differences among the courts of appeal remains an open question. But, regardless, it is now binding law in the Second Circuit, and its adoption of guiding non-dispositive factors should provide a roadmap for the resolution of similar litigation going forward. Such future developments may also be influenced by the Supreme Court's highly anticipated upcoming decision in *TransUnion LLC v. Ramirez*,[32] in which oral argument was held on March 30, 2021, addressing the closely related question of whether Article III or Federal Rule of Civil Procedure 23 permit a damages class action where the majority of the putative class did not suffer an actual injury. As always, Gibson Dunn remains available to help its clients in navigating this evolving area of the law.

---

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

[2] *Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019).

[3] *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020).

[4] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)).

[5] *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409–10 (2013).

[6] *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotation marks omitted).

[7] Allison Grande, *High Court FCRA Case Could Shake Up Class Action Standing*, Law360.com (Mar. 26, 2011), available at https://www.law360.com/articles/1368905/high-court-fcra-case-could-shake-up-class-action-standing.

[8] *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340 (11th Cir. 2021); *Beck. v.McDonald*, 848 F.3d 262, 273 (4th Cir. 2017).

[9] *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig*., 928 F.3d 42, 59 (D.C. Cir. 2019).

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

[11] *Reilly v. Ceridian Corp*., 664 F.3d 38, 45 (3d Cir. 2011).

[12] *In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017).

[13] *Tsao*, 986 F.3d at 1344.

[14] *Steven v. Carlos Lopez & Assocs., LLC*, 422 F. Supp. 3d 801, 802 (S.D.N.Y. 2019).

[15] *McMorris*, 2021 WL 1603808, at *1.

[16] *Id.* at *1 (quoting Amended Complaint ¶¶ 6, 34).

[17] *Steven*, 422 F. Supp. 3d at 807.

[18] *Id.* at 803.

[19] *Id.* at 804.

[20] *Id.* at 804–07.

[21] *Id.* at 807 (quoting *Clapper*, 568 U.S. at 416).

[22] *McMorris*, 2021 WL 1603808, at *3.

[23] *Id.* .

[24] *Id.* at *3 & n.2.

[25] *Id.*

[26] *Id.* at *5.

[27] *Id.*

[28] *Id.* at *6.

[29] *Id.*

[30] *Id.* at *6 n.7 (quoting *SuperValu*, 870 F.3d at 771).

[31] *Katz v. Pershing, LLC*, 672 F.3d 64, 80 (1st Cir. 2012).

[32] No. 20-297.

The following Gibson Dunn lawyers assisted in the preparation of this alert: Alexander H. Southwell, Akiva Shapiro, Jeremy S. Smith, Michael Nadler, and Eric Hornbeck.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any of the following members of the firm's Privacy, Cybersecurity and Data Innovation practice group, or the following authors:

Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Akiva Shapiro – New York (+1 212-351-3830, ashapiro@gibsondunn.com)

United States
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)

Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Related Capabilities

Privacy, Cybersecurity, and Data Innovation