Kilpatrick

May 25, 2022

Data breach class actions: Southern District of New York dismisses action against health care providers for lack of standing

by James F. Bogan III

Takeaway: In a prior article, we reported on the Second Circuit's decision in *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021), in which the court, ruling on an issue of first impression, set out a non-exhaustive three-factor test for determining whether allegations of injury flowing from a data breach rise to the level of a cognizable Article III injury-in-fact. *See Data breach class actions: Second Circuit sets out parameters for Article III injury-in-fact* (May 28, 2021). The Southern District of New York recently applied *McMorris* to dismiss a data breach class action in *Aponte v. Northeast Radiology, P.C.,* No. 21 CV 5883 (VB), 2022 WL 1556043 (S.D.N.Y. May 16, 2022), while acknowledging that the decision might not have survived the Supreme Court's ruling in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), that standing may not be based on "the mere risk of future harm." 2022 WL 1556043, at *3 (citation omitted); *see also SCOTUS standing ruling – "No concrete harm, no standing" – sidesteps class action issues and could limit federal subject matter jurisdiction over class actions* (June 30, 2021). Nevertheless, the district court applied *McMorris* because "it is the task of the Second Circuit, not this Court, to determine if *McMorris* should be overturned." 2022 WL 1556043, at *3 (quoting *Cooper v. Bonobos, Inc.*, 2022 WL 170622, at *3 n.1 (S.D.N.Y. Jan. 19, 2022)). The *Aponte* decision illustrates the shifting standards applicable to Article III standing in data breach actions in the Second Circuit and elsewhere.

In *Aponte*, Jose Aponte II and Lisa Rosenberg filed a putative class action against Northeast Radiology, P.C. ("Northeast Radiology") and Alliance HealthCare Services, Inc., alleging they failed to protect plaintiffs' "electronic protected health information" ("e-PHI") from unauthorized disclosure. 2022 WL 1556043, at *1. According to their complaint, Mr. Aponte and Ms. Rosenberg provided Northeast Radiology with their "names, addresses, dates of birth, gender, and medical history information," after which a hacker allegedly gained access to the computer servers on which the data were stored. *Id*.

Plaintiffs claimed a hacker accessed defendants' "Picture Archiving and Communications Systems" ("PACS") and was thereby "presented with a list of all [patient] studies and the number of related images stored on [defendants'] PACS," consisting of "approximately 62 million images associated with 300,000 patients." *Id*. (quoting amended complaint). This, plaintiffs said, gave the hacker access to highly sensitive e-PHI, "including patient name, date of birth, patient ID (which plaintiffs allege often corresponds to social security number), date of examination, and study description, …" *Id*. They further alleged that the "PACS failed to include basic

security features like encryption or passwords, and the list of file names containing e-PHI could be downloaded and saved" by the hacker. *Id*.

After the breach, Northeast Radiology issued a press release explaining that the data of at least twenty-nine patients was accessed but that it was "unable to determine if other patients' information on the system was also compromised." *Id*.

According to Mr. Aponte and Ms. Rosenberg, "they face[d] an ongoing imminent risk of identity theft and fraud because, unlike a credit card, there is no way to cancel e-PHI," requiring them "to continuously monitor their accounts, purchase credit and identity theft monitoring services, and expend additional time and effort to prevent and mitigate potential future losses." *Id*. Plaintiffs alleged that "they would not have used defendants' services had they known defendants did not employ reasonable security measures" and that they suffered an Article III injury in the form of an "intrusion upon their seclusion," given "defendants' insufficient security practices made plaintiffs' data available for unauthorized access." *Id.* at *1-*2. They asserted claims for negligence, negligence per se, breach of contract, breach of implied contract, violations of New York General Business Law Section 349, and "intrusion upon seclusion." *Id*. at *2.

The *McMorris* three-factor test poses the following questions: "(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." *Id*. at *3 (quoting *McMorris*, 995 F.3d at 303)). Applying this test, the *Aponte* court rejected the four arguments advanced by the plaintiffs that they had suffered an injury-in-fact.

First, the plaintiffs did not "face a substantial and imminent risk of fraud and identity theft," given that they did not assert that "third parties misused or attempted to misuse their data." Id. And because they were not "members of the group of twenty-nine patients whose information was determinedly accessed," their claim of data access constituted "conjecture." *Id*.

Second, the court rejected their allegation that they "will be required to spend substantial amounts of time monitoring their accounts for identity theft and fraud," given that they cannot manufacture an Article III injury by "protecting [themselves] against [a] speculative threat." *Id*. at *3-*4 (quoting *McMorris*, 995 F.3d at 304 n.7).

Third, the court rejected their argument that "they would not have sought defendants' services had they known the nature of defendants' data security practices," *id*. at *3, because "[i]f plaintiff[s] bargained for data security, and no third party has misused [their] data, then plaintiff[s] ha[ve] received exactly what [they] paid for." *Id*. at *4 (citation omitted).

Fourth, the court rejected plaintiffs' argument that "defendants' conduct caused unauthorized access by third parties that intruded upon plaintiffs' seclusion," *id*. at *3, because "it [was] not defendants who improperly accessed plaintiffs' data, but instead other, unauthorized third parties." *Id*. at *5.

Finally, the court dismissed the plaintiffs' claims for statutory violations, "because plaintiffs have failed to allege a concrete injury-in-fact arising from the breach." *Id.*