Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

2nd Circ. Clarifies Data Breach Injury Standing Threshold

By **Dorothy Atkins**

Law360 (April 26, 2021, 9:04 PM EDT) -- The Second Circuit on Monday clarified that the risk of identity theft after a data breach may be grounds to sue, but affirmed the dismissal of a proposed class action against a veteran's health services company over an accidentally sent email that contained workers' Social Security numbers, saying it fell short.

In a 21-page opinion, a unanimous three-judge panel held that plaintiffs may establish Article III constitutional standing based on the theory that the breach put them at an increased risk of identity theft or fraud, if the data is sensitive and has been misused or if there is reason to believe it will be misused.

However, the panel said in the instant suit, plaintiff Devonne McMorris didn't show that her personal identifiable information, or PII, had been compromised in a way that met this bar.

"Because McMorris did not allege that her PII was subject to a targeted data breach or allege any facts suggesting that her PII (or that of any others) was misused, the district court correctly dismissed her complaint for failure to establish an Article III injury in fact," the opinion says.

The ruling marks an end to a proposed class action that McMorris, Sean Mungin and Robin Steven filed in July 2018 against the veteran mental health services provider Carlos Lopez & Associates LLP, which contracts with the U.S. Department of Veterans Administration in Lincoln, Maine, and its owner, Carlos Lopez.

The workers sued after an employee accidentally sent a companywide email to approximately 65 workers that had a spreadsheet containing personal information — including Social Security numbers, home addresses, dates of birth, telephone numbers, educational degrees and dates of hire — of roughly 130 current and former employees.

The workers accused the employer of negligence and violating consumer protection statutes in California, Florida, Texas, Maine, New Jersey and New York. Although the complaint doesn't allege the workers' identities were stolen, they claim they were harmed because they had to spend time canceling credit cards, considering applying for new Social Security numbers and buying credit monitoring and identity theft protection services.

In December 2018, the employer filed a motion to dismiss, arguing the workers weren't injured by the

email and therefore they didn't have standing to sue. But before the trial judge ruled on the motion, the parties struck a settlement.

In a hearing on the proposed deal, U.S. District Judge Jesse M. Furman said he was inclined to dismiss the case, because there was no evidence that the employees' identities were actually stolen or misused and the disclosures appeared to be accidental and not malicious.

The judge ultimately denied the settlement in November 2019, finding he didn't have jurisdiction over the dispute because the workers didn't have standing to sue, and adding it was "arguably a misnomer to even call this case a 'data breach' case," since, "at best, the data was 'misplaced.'"

McMorris appealed the denial, but on Monday, the Second Circuit panel rejected the appeal.

The panel said it agrees with sister circuits that have found plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of sensitive data if those breaches were the result of targeted attacks or if some of the data was misused.

However, the panel concluded the workers in the instant suit haven't shown they are at an increased risk of identity theft, and the cost of taking proactive measures to prevent future identity theft aren't enough to constitute an injury in fact.

"Where plaintiffs 'have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury,'" the opinion says. "This notion stems from the Supreme Court's guidance in Clapper, where it noted that plaintiffs 'cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.'"

The workers' counsel, Abraham Z. Melamed of Derek Smith Law Group PLLC, said in a statement Monday that the ruling is a significant victory for data breach victims.

"While we are not pleased with the fact-specific outcome of the court's decision and will evaluate our options relating to it, we are happy that the court held that an increased risk of future injury in a data breach case may constitute a sufficient injury for Article III standing, and that the court articulated a framework for judges to evaluate in assessing that standing," he said.

Counsel for the employer didn't immediately respond Monday to requests for comment.

Judges Richard J. Sullivan, Guido Calabresi and Robert Katzmann sat on the panel for the Second Circuit.

The workers are represented by Abraham Z. Melamed of Derek Smith Law Group PLLC.

Carlos Lopez & Associates and Lopez are represented by Joseph R. Palmore, Michael B. Miller, Lena H. Hughes and Janie Buckley of Morrison & Foerster LLP.

The case is Devonne McMorris et al. v. Carlos Lopez & Associates LLC et al., case number 19-4310, in the U.S. District Court of Appeals for the Second Circuit.