MAY 28, 2021

Data breach class actions: Second Circuit sets out parameters for Article III injury-in-fact

by James F. Bogan III

Takeaway: Since the U.S. Supreme Court addressed the issue of standing based on allegations of possible future injury in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), the courts of appeals have addressed this standing issue in a number of data breach cases. In *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021), the Second Circuit, 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. The *McMorris* decision may be the most useful circuit decision to date on the injury-in-fact issue, as it provides a workable framework for standing that likely will be applied in data breach cases for years to come.

In *McMorris*, an employee of Carlos Lopez & Associates, LLP ("CLA"), inadvertently sent an e-mail to all of CLA's employees attaching a spreadsheet containing the personally-identifiable information ("PII") – including social security numbers – of over 100 current and former CLA employees. Soon thereafter, CLA notified its current employees about the inadvertent disclosure, but it did not contact any of its former employees or take any other steps to address the disclosure.

Three individuals whose PII had been disclosed then filed a putative class action suit against CLA and its principal, alleging claims for negligence, negligence *per se*, and consumer protection claims on behalf of putative classes in California, Florida, Maine, New Jersey, New York, and Texas. They alleged that CLA violated its duties to safeguard their PII and take reasonable steps to limit the damage caused by the disclosure. "[W]hile they did not allege that the PII in the spreadsheet was ever shared with anyone outside of CLA or taken or misused by any third parties, Plaintiffs claimed that they cancelled credit cards, purchased credit monitoring and identity theft protection services, and spent time assessing whether they should apply for new Social Security numbers after the email incident." *Id*. at 298.

CLA moved to dismiss the claims for lack of Article III standing but the parties later agreed to a class settlement, joining in a motion to preliminarily approve the settlement. At the fairness hearing, the district court advised the parties of its view that it did not have jurisdiction and thus could not approve the settlement, given that the plaintiffs had not suffered an injury-in-fact and lacked Article III standing to press their claims. Soon thereafter, the district court entered an order dismissing the plaintiffs' claims, ruling (among other grounds) that plaintiffs "failed to allege facts indicating that they faced 'certainly impending' identity theft or fraud, or even a 'substantial risk' of such harm." *Id*. at 299. The court further ruled that "since Plaintiffs failed to allege a substantial risk of identity theft or that such harm was certainly impending, they could not establish standing by, in essence, inflicting harm on themselves [by spending time and money dealing with PII disclosure] based on a speculative fear of future identity theft." *Id.* The district court dismissed the case. One of the named plaintiffs appealed, and the Second Circuit affirmed the district court's ruling.

The sole issue on appeal concerned the sufficiency of plaintiffs' allegations they had suffered an Article III injury-in-fact. As the Second Circuit observed, the leading case on this point is *Clapper*, where the Supreme Court ruled that "allegations of possible future injury" – including an "objectively reasonable likelihood" of future injury – do not clear the injury-in-fact hurdle. Id. at 300 (quoting *Clapper*, 568 U.S. at 409–10). "Rather, a future injury constitutes an Article III injury in fact only 'if the threatened injury is *certainly impending,* or there is a *substantial risk* that the harm will occur.'" *Id*. (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)) (emphasis added).

Recognizing the issue as one of first impression in the Second Circuit, and reviewing data breach decisions from other circuits on the issue of standing, the panel stated: "We therefore join all of our 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." *Id*. at 300-301 (emphasis added). But the key Article III issue, according to the panel, concerns the nature and quality of allegations supporting any "increased risk" theory, to determine whether the allegations show a *substantial risk* of future injury.

According to the panel, and based on the rulings of other circuit courts, three factors drive the injury-in-fact analysis:

"First, and most importantly, our sister circuits have consistently considered whether the data at issue has been compromised as the result of a targeted attack intended to obtain the plaintiffs' data." *Id*. at 301. Regarding this factor, an allegation that cybercriminals targeted and stole the plaintiffs' PII would show a substantial risk of future injury.

"Second, while not a necessary component of establishing standing, courts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused – even if plaintiffs' *particular* data subject to the same disclosure incident has not yet been affected." *Id.* (emphasis in original). Regarding this factor, an allegation that stolen PII has been placed on the "Dark Web" would qualify as an injury-in-fact.

Third, "courts have looked to the type of data at issue, and whether that type of data is more or less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed. Naturally, the dissemination of high-risk information such as Social Security numbers and dates of birth – especially when accompanied by victims' names – makes it more likely that those victims will be subject to future identity theft or fraud." *Id.* at 302.

The panel then set out its own three-factor test, while emphasizing the fact-intensive nature of any injury-in-fact analysis: "We therefore hold that courts confronted with allegations that plaintiffs are at an increased risk of identity theft or fraud based on an unauthorized data disclosure should consider the following non-exhaustive factors in determining whether those plaintiffs have adequately alleged an Article III injury in fact: (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 303.

As for allegations of injury based on time and money spent dealing with a data breach, the panel reiterated the key consideration as whether the allegations suffice to show a substantial risk of future injury. A showing of a substantial risk allows recovery of reasonable expenses incurred in mitigating that

risk. Returning to the Supreme Court's decision in *Clapper*, the panel said that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* at 303 (quoting *Clapper*, 568 U.S. at 416).

Turning to plaintiffs' allegations, the panel easily concluded that they had not alleged a cognizable injury-in-fact: "First, Plaintiffs never alleged that their data was intentionally targeted or obtained by a third party outside of CLA. ... Second, Plaintiffs do not allege that their data (or the data of any other then-current or former CLA employees) was in any way misused because of the accidental email. ... Finally, while the information that was inadvertently disclosed by CLA included the sort of PII that might put Plaintiffs at a substantial risk of identity theft or fraud, in the absence of any other facts suggesting that the PII was intentionally taken by an unauthorized third party or otherwise misused, this factor alone does not establish an injury in fact." *Id.* at 303-04.

Accordingly, the Court of Appeals affirmed the district court's determination that it had no jurisdiction to approve the class settlement and therefore properly dismissed the case for lack of Article III standing. *Id.* at 305.