Jun 2022 | Articles Blog: The Westchester Litigator

My Identity Could Be Stolen . . . At Some Point!: An Analysis of Federal Standing and Future Harm in Data Breach Cases

It is axiomatic that plaintiffs in federal court must have standing under Article III of the Constitution to bring their claims. To demonstrate standing, plaintiffs must show, *inter alia*, that they have suffered an "injury-in-fact," which the Supreme Court has defined as "an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." Although the Second Circuit considers the injury-in-fact requirement to have a low threshold, it has proven problematic in the data breach context, where it is often unclear if or when a plaintiff's stolen personal data will be used for harmful purposes. A recent case before the Southern District of New York analyzes this situation and demonstrates how challenging it can be to establish an injury in fact where the only injury is the future risk of identity theft.

The Case: *Aponte v. Northeast Radiology, P.C.*

In *Aponte v. Northeast Radiology, P.C.*, Index No. 5883/2022 (S.D.N.Y. May, 16 2022), the plaintiffs brought suit claiming the defendants failed to protect the plaintiffs' electronic protected health information ("e-PHI") after an unauthorized individual accessed the defendants' computer servers. Following the breach, the defendants announced that 29 patients' information was accessed. Although they were not among that 29 and had no evidence that the compromised data had been misused, the plaintiffs brought suit alleging they suffered an injury-in-fact because of the future risk of identity theft and fraud.

To determine whether the plaintiffs had standing, Judge Vincent Briccetti applied the three-factor test articulated by the Second Circuit in *McMorris v. Carlos Lopez & Assocs., LLC*: 1) whether the plaintiffs' data had been exposed as the result of a targeted attempt to obtain that data; 2) whether any portion of the dataset had already been misused, even if the plaintiffs themselves had not yet experienced identity theft or fraud; and 3) whether the type of data that had been exposed is sensitive such that there is a high risk of identity theft or fraud.

While acknowledging that plaintiffs in cyber fraud cases "need not wait until they suffer identity theft to bring their claims," the Court concluded that the plaintiffs' allegations of future harm were too remote and speculative to confer standing. Judge Briccetti reasoned that because the plaintiffs did not allege any misuse or attempted misuse of their data resulting from the breach, and as they could not prove the files containing their e-PHI were downloaded, saved or viewed by the unauthorized users, the plaintiffs' allegations were insufficient to establish an actionable risk of future harm.

Because the plaintiffs did not sufficiently allege they had suffered an injury-in-fact or would so suffer in the future, the Court concluded the plaintiffs' failed to establish standing to bring their claims and thus granted the defendants' motion to dismiss pursuant to Rule 12(b)(1) for lack of subject matter jurisdiction.

Takeaway

With the rise of cyber fraud comes the rise of lawsuits by plaintiffs who allege their personal information has been compromised and may be misused in the future. It is not enough, however, to allege that a data breach has occurred. Rather, to have standing to maintain a claim, a plaintiff must allege facts supporting a substantial and concrete risk of future harm. Attorneys on both sides of cyber fraud matters should pay careful attention to the federal standing requirements in drafting and responding to data breach-related claims.