Articles + Publications | May 13, 2021

Second Circuit Clarifies Article III Standing Threshold for Data Breach Class Actions

WRITTEN BY

Angelo A. Stio III | Jan P. Levine | Jason J. Moreira

The Second Circuit recently issued a decision in *McMorris v. Carlos Lopez & Associates, LLC*, No. 19-4310, 2021 U.S. App. LEXIS 12328 (2nd Cir. Apr. 26, 2021), which clarifies the circumstances under which plaintiffs alleging an increased risk of future identity theft or fraud due to the exposure of their personal data can establish Article III standing. Notable for being the first Second Circuit decision to address privacy-related standing questions that had arguably created a circuit split, the court endorsed a three-factor framework that would reject a finding of Article III standing absent sufficient evidence of "increased risk" of future fraud or identity theft, but which left open the possibility that standing could still be established where plaintiffs allege a sufficient likelihood of misuse of their personal data.

Factual Background

In *McMorris*, an employee of defendant Carlos Lopez & Associates (CLA), a provider of mental health services for veterans, inadvertently emailed a spreadsheet containing personally identifiable information (PII) of approximately 130 current and former CLA employees to all other current employees of CLA. The plaintiffs then sued CLA for negligence and violation of state consumer protection laws.

The district court found that the plaintiffs had not alleged that their PII had actually been misused or compromised as the result of, for example, a hacking incident or data breach by a malicious third party, but had at best demonstrated that their data had been internally "misplaced" by the CLA employee who inadvertently disseminated the spreadsheet. In addition, the district court rejected the plaintiffs' claim that time spent cancelling their credit cards or otherwise monitoring or changing the information on their financial accounts due to the inadvertent disclosure of the spreadsheet could constitute injury sufficient to give rise to Article III standing, finding that the plaintiffs' efforts to mitigate the potential future misuse of their PII were self-imposed and based on a speculative fear of future identity theft. As a result, the district court found that the plaintiffs lacked standing and dismissed the case for lack of subject matter jurisdiction.

The Second Circuit's Decision

The Second Circuit affirmed the trial court's decision. However, it left open the possibility that under the right set of facts, the plaintiffs could conceivably establish standing provided that they could demonstrate a sufficiently increased risk of identity theft flowing from the unauthorized disclosure of their data. In so holding, the Second Circuit explicitly endorsed a nonexclusive three-factor test utilized by other courts for assessing whether the risk of harm associated with an alleged data breach is sufficiently concrete, particularized, and imminent to support a

finding of Article III standing:

1. Whether the plaintiff's data has been exposed as the result of a targeted attempt to obtain that data, such as a hacking incident or data breach by a malicious third party;

2. Whether any portion of the data acquired had already been misused, even if the plaintiffs themselves had not yet been the subjects of identity theft or fraud; and

3. Whether the type of data that has been exposed is of such a sensitive nature that the risk of identity theft or fraud is heightened.

Each of these factors is designed to probe the central question of assessing the likelihood of future harm. For example, absent allegations or evidence that an unauthorized third party intentionally sought out and obtained the plaintiffs' personal data (as opposed to that data having been mistakenly disclosed), the court noted that the risk of future identity theft may be found too speculative to support Article III standing. Similarly, if other individuals' data from within the same dataset has already been misused (even if the plaintiffs' data has not), or if the type of data alleged to have been exposed is particularly sensitive — such as the plaintiffs' names, Social Security numbers, and dates of birth — the court noted that the likelihood of future harm would be greater, and there will be stronger grounds to support Article III standing. The Second Circuit's approach in *McMorris* is therefore in line with the standard for establishing injury-in-fact currently recognized by the Supreme Court, which is that "an allegation of future injury may suffice" to establish Article III standing if the threatened injury is "certainly impending," or there is a "substantial risk" that the harm will occur.

Takeaways

McMorris has major implications for companies seeking to defend against claims arising from a data breach. On the one hand, by endorsing the three-factor test adopted by other courts, the Second Circuit arguably provides guidance to prospective plaintiffs on how to structure their claim — or at least which facts to emphasize — to maximize the likelihood that Article III standing will be found. On the other hand, however, the court's refusal to recognize credit monitoring and other prophylactic efforts as indicia of future harm demonstrates that prospective plaintiffs cannot "manufacture" standing using "self-help" methods. Similarly, under the Second Circuit's framework, the exposure of sensitive data that is inadvertent or otherwise not the result of a targeted, malicious hacking incident or data breach may be less likely to confer standing.

With all of this in mind, a company's response to a security incident is essential in minimizing the risk of litigation. A prompt investigation, timely notice, and offering credit monitoring and identity theft protection when required are helpful prophylactic mechanisms to address claims of future harm and demonstrate no Article III standing exists.

With all of this in mind, a thoughtful and strategic response to a security incident is essential to minimize exposure to litigation and a regulatory inquiry. Angelo A. Stio III, Jan P. Levine, and Jason J. Moreira are members of Troutman Pepper Hamilton Sanders LLP's Cybersecurity, Information Governance, and Privacy Group, an interdisciplinary group of attorneys that help clients address actual or suspected security incidents, understand legal obligations, respond to regulatory inquiries and defend against class actions.

RELATED INDUSTRIES + PRACTICES

- Business Litigation
- Consumer Financial Services
- Health Care + Life Sciences
- Privacy + Cyber
- White Collar Litigation + Investigations