

Second Circuit Dismisses Privacy Suit, But Rules That Claimants Can Sue For Increased Risk Of Identity Theft From Data Breach

05.27.21



(Article from *Insurance Law Alert*, May 2021)

For more information, please visit the [Insurance Law Alert Resource Center](#).

The Second Circuit ruled that individuals have Article III standing to sue over the unauthorized release of their personal information, even if they have not yet been the victims of identity theft. Nevertheless, the court dismissed the class action suit seeking damages based on an “increased risk” of identity theft, finding that the plaintiffs had not met their burden of establishing injury-in-fact. *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021).

An employee accidentally sent an email to approximately 65 other employees that included a spreadsheet containing sensitive personal information of more than 100 current and former employees. Thereafter, three employees filed a class action suit against the company, alleging negligence and statutory violations. While the complaint did not allege any instances of fraud or identity theft as a result of the email, it claimed that the employees were at an increased risk of identity theft and had incurred costs associated with the cancellation of credit cards and the purchase of credit monitoring services, among other things. A New York federal district court dismissed the suit based on a lack of Article III standing, finding that the plaintiffs had failed to allege any “concrete and particularized” injury. The Second Circuit affirmed.

Addressing this matter of first impression, the Second Circuit held that a plaintiff can establish standing based on a risk of future identity theft stemming from an unauthorized disclosure of personal information. It recognized that other federal circuit courts have held that actual misuse following a data breach is not necessary to establish standing. However, the court ruled that here, plaintiffs had not adequately alleged facts sufficient to establish standing based on an “increased risk” theory, noting that the complaint did not allege any “impending” injury or “substantial risk that the harm will occur.” The court emphasized that the data-compromise was not the result of a targeted, purposeful act and that none of the employees’ data had actually been misused.

Finally, the court ruled that costs incurred by the plaintiffs in taking measures to protect themselves from future identity theft did not constitute an injury-in-fact. The court explained that “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.”

