WIGGIN
WIGGIN AND DANA

ADVISORY

AUGUST 29, 2023

SECOND CIRCUIT RULING CLARIFIES THRESHOLD REQUIREMENTS FOR DATA BREACH LAWSUITS

If you have any questions about this Advisory, please contact:

DAVID HALL
215.988.8325
dhall@wiggin.com

NATHAN GUEVREMONT
203.498.4367
nguevremont@wiggin.com

The Second Circuit recently issued an opinion that may move up the timeline for class action lawsuits following data breaches and help chart a course for plaintiffs seeking to establish that they have standing to sue immediately following such breaches. The court also reached several conclusions that will be critical points to consider for companies seeking to mitigate the fallout from data breaches in the future.

BACKGROUND

In *Bohnak v. Marsh & McLennan Companies, Inc.*, plaintiff Nancy Bohnak sued Marsh & McLennan Companies, Inc. (MMC) and its subsidiary for negligence, breach of implied contract, and breach of the MMC's duty of confidentilaity following a data breach. Bohnak alleged that MMC stored private information, including names and social security numbers, for at least 7,000 individuals including its current or former employees, clients, and investors. An unnamed bad actor was able to access that private information using a vulnerability in third-party software used by MMC.

Bohnak did not claim that the bad actor had yet used any of her (or the class's) private information. Instead, she argued that the disclosure itself constituted an injury, and the breach created a likelihood of future injury if the bad actor exploited her private information. She claimed she thus incurred expenses to monitor and protect against identity theft and fraud.

MMC moved to dismiss. It argued that Bohnak could not establish that she had any actual damages and she lacked Article III standing to sue because she was unable to allege that any stolen data had been used to her detriment. Under Article III of the Constitution, federal courts only have jurisdiction to decide "cases" and "controversies." As a result, plaintiffs must show that they have "standing" under Article III by establishing (1) that they suffered an injury in fact that is "concrete, particularized, and actual or imminent"; (2) that the defendant caused the injury; and (3) that the injury is likely redressable by a court. *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020). MMC asserted that Bohnak failed at the first step. Although the district court held that Bohnak did have standing to sue, it concluded that she had no cognizable claim for damages and dismissed her complaint.

CONTINUED

SECOND CIRCUIT RULING CLARIFIES THRESHOLD REQUIREMENTS FOR DATA BREACH LAWSUITS

THE SECOND CIRCUIT'S DECISION

The Second Circuit reversed the trial court's dismissal. In a unanimous opinion authored by Judge Beth Robinson, the Second Circuit explained that Bohnak's allegations were sufficient to establish standing in two ways, and that Bohnak thereby necessarily showed that she had cognizable damages.

First, the court noted that in *TransUnion, LLC v. Ramirez*, 141 S. Ct. 2190 (2021), the Supreme Court recognized that a plaintiff may establish a "concrete harm" even without showing an immediate physical injury or monetary loss. That is, a plaintiff may establish standing through an intangible harm where the plaintiff shows that the alleged harm bears a "close relationship" to a harm "traditionally recognized as providing a basis for a lawsuit in American courts." Here, the Second Circuit explained, Bohnak's allegation that MMC negligently allowed a bad actor to access her name and social security number was sufficiently similar to the traditional tort of "public disclosure of private facts" to establish that she had standing. The court emphasized that its analysis applied even though Bohnak had not (and possibly could not) bring an actual claim for "public disclosure of private facts." All that mattered was that the intangible harm she alleged arising out of the data breach had a close relationship to a traditionally recognized injury.

Second, the court held that Bohnak's allegations were sufficient to establish a "concrete harm" in another way: she alleged that she incurred out-of-pocket expenses after the breach to prevent or detect potential identify theft. Reaffirming its earlier decision in *McMorris v. Carlos Lopez & Associates*, 995 F.3d 295 (2d Cir. 2021), the Second Circuit confirmed that, when a plaintiff shows a "substantial risk of future identity theft or fraud," any expense they reasonably incur to avoid that risk constitutes a concrete injury in fact. That holding comports with recent decisions from the First and Third Circuits, holding that time and expense incurred to avoid further financial injury following a data breach represented concrete harms for purposes of standing.

Next, the Second Circuit held that the harm Bohnak alleged was sufficiently "imminent" to support Article III standing. A harm is "imminent" under Article III when the "threatened injury is certainly impending, or there is a substantial risk that the harm will occur." In *McMorris*, the Second Circuit identified three factors that courts should consider to make this inquiry in cases where private information is inadvertently or wrongfully disclosed: (1) whether the disclosure was the result of a targeted attack, making future identity theft or fraud more likely; (2) whether there is evidence or allegation that some portion of the disclosed information was already wrongfully misused, making it more likely that the plaintiff's information would be similarly misused as well; and (3) whether the disclosed information is the type (like social security numbers) that creates a higher risk of identity theft or fraud. Here, the first and third factors weighed heavily in favor of concluding that there was an "imminent" harm to Bohnak. The second factor weighed against imminence, but the Second Circuit emphasized that it was not dispositive, particularly where the other factors were more compelling. As a result, Bohnak had established that her injuries from the data breach were "actual or imminent" as required to establish Article III standing.

Finally, the court reversed the district court's determination that Bohnak had failed to establish that she had any cognizable damages. The Second Circuit held that a plaintiff who

CONTINUED

SECOND CIRCUIT RULING CLARIFIES THRESHOLD REQUIREMENTS FOR DATA BREACH LAWSUITS

establishes an injury in fact for standing purposes necessarily also establishes the availability of damages for that injury. Here, Bohnak went one step further by also alleging that she spent time and money to mitigate the consequences of MMC's data breach. The court therefore reversed the district court's judgment dismissing Bohnak's claims and remanded for further proceedings.

KEY TAKEAWAYS

In concluding that Bohnak's allegations were adequate to establish Article III standing and show cognizable damages, the Second Circuit reached several conclusions that are significant for companies facing future data breaches:

1. **Plaintiffs need not wait until their data is used to their detriment to sue based on a data breach that resulted from a targeted attack.**

   The Second Circuit's decision makes clear that individuals whose data is stolen in a targeted attack may sue *immediately* based on that breach and their risk of future harm.

2. **Where a data breach is the result of inadvertent disclosure on the part of the company, plaintiffs may face additional hurdles to establish standing.**

   The Second Circuit in *Bohnak* reaffirmed much of the reasoning in its earlier decision in *McMorris*. There, the court held that a plaintiff lacked standing to sue when their private information was inadvertently sent in a company-wide email. Applying the three-factor test from above, the court held that the plaintiff had not established a risk of "imminent" harm where the circumstances of the breach did not suggest the private data would be misused and there was no actual evidence or allegation of misuse.

3. **The three-factor test from *McMorris* still applies in evaluating the risk of future harm in the Second Circuit.**

   In *Bohnak*, the Second Circuit acknowledged some confusion among litigants over whether its earlier decision in *McMorris* still applied after the Supreme Court's decision in *TransUnion*. The Second Circuit held that, in most circumstances, it does. While the Supreme Court's decision in *TransUnion* provides guidance on whether an injury is "concrete," the test from *McMorris* helps courts determine whether an alleged future injury is sufficiently "imminent." As a result, businesses facing data breach suits must carefully evaluate both cases to assess possible standing arguments.

4. **When plaintiffs establish standing to sue following a data breach, they necessarily establish that they have suffered cognizable damages.**

   The district court in *Bohnak* held that Bohnak's allegations were sufficient to establish Article III standing, but dismissed her complaint because it concluded that she had no cognizable damages. The Second Circuit swiftly rejected that reasoning, adopting the Seventh Circuit's holding that, "To say that plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available." As a result, where a plaintiff has standing, courts in the Second Circuit must generally assume that they have alleged cognizable damages as well.