Kilpatrick

OCTOBER 27, 2022

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

by James F. Bogan III

Takeaway: We have written a number of articles about the kinds of intangible injuries that confer Article III standing in the data breach and credit reporting contexts. *See Data breach class actions: Southern District of New York dismisses action against health care providers for lack of standing* (May 25, 2022); *SCOTUS standing ruling – "No concrete harm, no standing" – sidesteps class action issues and could limit federal subject matter jurisdiction over class actions (June 30, 2021); and Data breach class actions: Second Circuit sets out parameters for Article III injury-in-fact* (May 28, 2021). The Third Circuit recently became the latest federal appellate court to examine the parameters for data breach standing in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022).

As a condition of her employment, Jennifer Clemens had to disclose sensitive personal and financial information to ExecuPharm, Inc. ("ExecuPharm"), including her social security number, passport, financial and bank account numbers, and personal family information. ExecuPharm in turn promised that it would "take appropriate measures to protect the confidentiality and security" of that information. 48 F.4th at 150.

But after Ms. Clemens departed ExecuPharm, the notorious hacking group known as CLOP accessed ExecuPharm's servers, exfiltrating sensitive employee information (including Ms. Clemens'), installing malware to encrypt the data, and demanding a ransom to decrypt the data. At some point, CLOP posted the data stolen from ExecuPharm on "the Dark Web" (including Ms. Clemens' data), making it available to criminal elements intent on purchasing stolen data to commit financial fraud. *Id.*

ExecuPharm provided periodic notices to its current and former employees, informing them of the hack and advising them to take precautionary measures, further notifying them that "[u]nauthorized access to [the compromised] information may potentially lead to the misuse of [their] personal data to impersonate [them] and/or to commit, or allow third parties to commit, fraudulent acts such as securing credit in [their] name." *Id.* at 151. Ms. Clemens did take precautionary measures, including reviewing her credit records, installing fraud alerts on her credit reports, moving her bank account to a new bank, and buying credit-monitoring services. *Id.*

In 2020, she filed a putative class action against ExecuPharm and its parent corporation in the Eastern District of Pennsylvania, alleging claims the Third Circuit panel categorized as claims for contract (breach of implied contract and breach of contract), tort (negligence and negligence per se), and secondary contract (breach of fiduciary duty and breach of confidence). ExecuPharm moved to dismiss Ms. Clemens' complaint and the district court granted the motion, ruling that Ms. Clemens' risk of future harm from the breach "was not imminent, but 'speculative,' because she had not yet experienced actual identity theft or fraud," and further ruling that the monetary expenses she incurred to prevent that "speculative risk" did not amount to an Article III injury-in-fact. *Id.* Ms. Clemens appealed, and the Third

Circuit reversed and vacated the district court's ruling.

To establish standing in federal court, a plaintiff must show "(1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief." *Id.* at 152 (quoting *Thole v. U.S. Bank N.A.,* 140 S. Ct. 1615, 1618 (2020)). The Third Circuit panel focused its analysis on the first element, evaluating whether Ms. Clemens' alleged injuries were "imminent" and "concrete."

The panel acknowledged the Supreme Court's 2013 ruling in Clapper that "a 'possible future injury' – even one with an 'objectively reasonable likelihood' of occurring – is not sufficient" to confer standing. *Id*. at 153 (quoting *Clapper v. Amnesty Int'l USA* , , 568 U.S. 398, 409-10, 414 n.5 (2013)). The panel then identified three "non-exhaustive factors [to] serve as useful guideposts, with no single factor being dispositive," in assessing whether an alleged injury is sufficiently "imminent" to confer standing: (1) "whether the data breach was intentional," (2) "whether the data was misused," and (3) "whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft." *Id*. at 153-54.

In evaluating whether an alleged injury is concrete, the panel divided the analysis into two steps. Citing the Supreme Court's decisions in *Spokeo, Inc. v. Robins,* 578 U.S. 330 (2016) and *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), the panel explained that "[t]he first step in assessing concreteness is to ask whether the asserted harm is adequately analogous to a harm traditionally recognized as giving rise to a lawsuit." *Id*. at 154. Although alleged data breach injuries are "intangible," "if the theory of injury is an unauthorized exposure of personally identifying information that results in an increased risk of identity theft or fraud, that harm is closely related to that contemplated by privacy torts that are 'well-ensconced in the fabric of American law.'" *Id*. at 155 (quoting *In re Horizon Healthcare Servs. Inc. Data Breach Litig*., 846 F.3d 625, 638-39 (3d Cir. 2017)).

The second step – as articulated by *TransUnion* – focuses on "the type of relief sought." *Id*. The panel held that "in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Id*. at 155-56.

Applying these standing principles, the panel held Ms. Clemens had Article III standing to assert her data breach claims: "she has alleged a future injury – the risk of identity theft or fraud – that is sufficiently imminent. The breach was conducted by a known hacking group CLOP, which intentionally stole the information, held it for ransom, and published it to the Dark Web, thereby making it accessible to criminals worldwide. The nature of the information – a combination of personal and financial data – is the type that can be used to perpetrate identity theft or fraud. Given that intangible harms like the publication of personal information can qualify as concrete, and because plaintiffs cannot be forced to wait until they have sustained the threatened harm before they can sue, the risk of identity theft or fraud constitutes an injury-in-fact." *Id*. at 159.