wiley

NEWSLETTER

CareFirst Asks the Supreme Court to Reaffirm Article III Standing Requirements in Cases of Data Breach

November 2017

On October 30, 2017, CareFirst filed a petition for a writ of certiorari asking the Supreme Court of the United States to review an August 2017 ruling by the U.S. Court of Appeals for the District of Columbia Circuit that found plaintiffs had Article III standing in a suit stemming from a 2015 data breach. The case would give the Court an opportunity to apply Article III principles – which limit judicially cognizable harms to concrete, particularized, and actual or imminent injury – in the context of a data breach.

In June 2014, CareFirst suffered a data breach in which attackers allegedly stole its customers' personal information. A group of CareFirst customers brought a class action in district court alleging 11 different state law causes of action, including negligence, breach of contract, and the violation of state consumer-protection statutes. CareFirst moved to dismiss for lack of Article III standing. The district court granted the motion, holding that the CareFirst customers alleged neither a present injury nor a high enough likelihood of future injury. The court reasoned that the plaintiffs' claim of harm – that they suffered an increased risk of identity theft because of the breach – was too speculative for Article III purposes.

The plaintiffs appealed to the U.S. Court of Appeals for the D.C. Circuit. The D.C. Circuit reversed the trial court's ruling and adopted the Seventh Circuit's reasoning in *Remijas v. Neiman Marcus Grp.* that data breaches create a risk of identity theft because the purpose of a hack is to eventually make fraudulent use of the obtained information. The court held that the alleged risk of identity theft was "substantial" because an unauthorized party had already accessed the data on

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

CareFirst's servers, and it was not merely speculative to infer that the attackers intended "to use that data for ill." Citing *Neiman Marcus*, the court was persuaded by the question of "[w]hy else would hackers break into a ... database and steal customers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities."

In its petition to the Supreme Court, CareFirst argues that the D.C. Circuit erroneously based Article III standing on asserted injuries that are conjectural and not imminent, violating principles that the Supreme Court espoused in *Clapper* and *Spokeo*. In *Clapper*, the Court specified that future injuries must be "certainly impending" and that "[a]llegations of possible future injury" are insufficient. In *Spokeo*, the Court held that a statutory violation, without actual harm, is not enough to confer standing, rejecting the argument that statutory violations are *de facto* concrete. Together, *Clapper* and *Spokeo* suggest that threat of harm based entirely on future possible acts of unknown third parties fails to satisfy Article III requirements.

As CareFirst notes in its petition, other circuits have held that plaintiffs must allege actual harm to satisfy Article III and that an increased risk of identity theft, without more, is insufficient. The Third, Fourth, and Eighth circuits have each held that plaintiffs lack standing based on an increased risk of identity theft without an allegation of actual injury.

CareFirst's petition highlights the uncertainty and importance of courts' evaluation of standing in the data breach context, noting that CareFirst itself has been subject to conflicting results in nearly identical cases brought against the company in different jurisdictions, even though the claims result from the same data breach. CareFirst's petition gives the Court an opportunity to address this uncertainty and specify how its standing doctrine applies in the data breach context.

Plaintiffs and defendants will be watching this case, which may invigorate plaintiffs seeking to sue companies after a data breach.

Shawn M. Donovan, co-author of this article, is a law clerk in Wiley Rein's Telecom, Media & Technology Practice.