D.C. Circuit Concludes Heightened Risk of Future Identity Theft Enough for Standing in Data Breach Class Action

Insights
8.15.17

Much to the dismay of companies, on August 1, 2017, the U.S. Court of Appeals for the D.C. Circuit made it easier for plaintiffs, and their attorneys, to bring class action data breach cases. In *Attias v. CareFirst, Inc.*, Case No. 16-7108, the Court concluded that the plaintiffs' heightened risk of future identity theft was sufficient to show standing at the pleading stage. With *CareFirst*, the D.C. Circuit becomes the second U.S. Court of Appeals to reach this conclusion. The 7th Circuit, in *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688 (7th Cir. 2015), was the first.

CareFirst represents further evolution of the U.S. Supreme Court's opinion in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). In *Spokeo,* the Supreme Court held that plaintiffs must allege more than a speculative harm. *Id.* at 1548. The harm must be "actual or imminent." *Id.*

In data breach cases, demonstrating "actual or imminent" harm at the pleading stage proves difficult. Often, plaintiffs' breached information has not yet been used to harm them. Companies have successfully used this fact, along with the reasoning in *Spokeo*, to challenge plaintiffs' standing to bring data breach claims early in the litigation. Such quick wins save companies hundreds of thousands of dollars. *CareFirst*, however, gives plaintiffs a path to defeating such challenges.

In *CareFirst,* the D.C. Circuit noted "that a plaintiff can establish standing [based on the risk of future injury] by satisfying *either* the 'certainly impending' test *or* the 'substantial risk' test." *CareFirst, Inc.* at *11 (citations committed). Proceeding under the "substantial risk" test, the Court stated that "[t]he . . . question, then, keeping in mind the light burden of proof the plaintiffs bear at the pleading stage, is whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach." *Id.*

Having framed the question, the D.C. Circuit then reasoned:

Here, . . . an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible— to infer that this party has both the intent and the ability to use that data for ill. As the 7th Circuit asked, in another data breach case where the court found standing, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *See Remijas v. Neiman Marcus Grp.,* 794 F.3d 688, 693 (7th Cir. 2015).

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.

Id. at * 14. The Court went on:

No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken. That risk . . . satisfies the requirement of an injury in fact.

Id.

Once the Court found that plaintiffs satisfied the injury in fact requirement, it quickly agreed that plaintiffs had sufficiently shown the final two standing elements outlined in *Spokeo*: (1) the injury in fact was "fairly traceable to the challenged conduct of the defendant" and (2) the injury was "likely to be redressed by a favorable decision." *CareFirst* at *14-15 (citing *Spokeo* at 136 S. Ct. at 1547). With that, the Court held that plaintiffs had standing to proceed with its data breach claims.

There is no doubt that *CareFirst* makes it more difficult for companies to challenge standing in data breach actions within the D.C. Circuit. Companies everywhere, however, must pay attention, as data breach matters easily cross and jump jurisdictional lines. Moreover, the D.C. Circuit joining the 7th Circuit starts a trend, which will likely lead to other U.S. jurisdictions concluding that a heightened risk of future identity theft is sufficient to show standing.

Companies used *Spokeo* as a quick out in data breach cases, which they still may do with some success. Nonetheless, plaintiffs will now use *CareFirst* to break through the motion to dismiss phase and move more quickly to class certification and discovery. It will result in increased litigation and settlement costs to companies. Needless to say, *CareFirst* leaves plaintiffs' attorneys everywhere with a smile.

Companies can avoid increased costs associated with cases like *CareFirst* through the design and implementation of effective privacy programs. By identifying and categorizing data based on its sensitivity, companies can design privacy programs that work to ensure that sensitive data, like Social Security numbers, is properly protected. This, in turn, reduces the probability of such data falling into the wrong hands, and thus, the likelihood of acquired data being of the type thieves can use to cause harm, regardless of whether a technical breach has occurred.

If you would like more information on how to setup and implement a privacy program which can help counter the effects of *CareFirst* and similar cases, please contact us.

Copyright © 2025 Fisher Phillips LLP. All Rights Reserved.