February 21, 2018

U.S. Supreme Court Declines to Review Standing of Data Breach Plaintiffs

Court Will Not Disturb the D.C. Circuit's Ruling in *CareFirst* Class Action, Allowing Plaintiffs to Proceed Based on a "Substantial Risk" of Harm, Rather than Actual Harm

SUMMARY

Yesterday, the U.S. Supreme Court denied *certiorari* in *CareFirst, Inc.* v. *Chantal Attias*, No. 17-641. In *CareFirst*, the U.S. Court of Appeals for the D.C. Circuit held that plaintiffs suing over a 2014 data breach had established standing by asserting there was a substantial risk that unauthorized access to their personal information, including credit card and social security numbers, could be used for identity theft, even if there were no allegations that such identity theft had occurred. The D.C. Circuit then concluded that, in the context of the exposure of credit card and social security numbers, a substantial risk of harm exists simply by virtue of the data beach and the nature of the data stolen.

BACKGROUND

In 2014, health insurer CareFirst suffered a cyberattack in which the personal information of approximately one million policyholders was stolen. A group of CareFirst policyholders brought a putative class action alleging that they suffered a heightened risk of identity theft as a result of the data breach. The district court dismissed the action for lack of standing, holding that plaintiffs' allegation of injury was too speculative, and that the plaintiffs did not allege how the data thieves could commit identity theft based on the information they accessed in the CareFirst breach.[1] The district court did not read the complaint to allege the theft of credit card and social security numbers.[2]

On appeal, the D.C. Circuit reversed, holding that a plaintiff need only show that it has suffered an "injury in fact" that is "fairly traceable" to the defendant's actions and that is "likely to be redressed" by the relief

sought.[3] Under the Supreme Court's decision in *Spokeo*, "injury in fact" must be concrete, particularized, and "actual or imminent" rather than speculative.[4] Following *Spokeo*, the CareFirst dispute centered on whether the plaintiffs' allegations of future injury are "actual or imminent."

Under this standard, the D.C. Circuit found that the plaintiffs had established standing by asserting there was a substantial risk that unauthorized access to their personal information would injure them. In particular, the D.C. Circuit disagreed with the District Court's determination that the plaintiffs had not alleged that plaintiffs' credit card and social security numbers had been stolen, something that substantially increased the risk of future identity theft.[5] As the D.C. Circuit noted, "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."[6]

The D.C. Circuit then distinguished the *CareFirst* plaintiffs' allegations from those in the U.S. Supreme Court's leading decision on the subject, *Clapper* v. *Amnesty International USA*, 568 U.S. 398, 409 (2013), in which plaintiffs alleged that it was likely the U.S. government would illegally monitor their conversations when they were speaking to individuals abroad. The D.C. Circuit noted that, in contrast to *Clapper*, an unauthorized party had already accessed the plaintiffs' personal information, including credit card and social security numbers.[7] Therefore, the court found the heightened risk of identity theft was much more substantial than the alleged harm in *Clapper*.[8] The court concluded that, in the context of alleged injury arising from a data theft, a substantial risk of harm exists "simply by virtue of the hack and the nature of the data [taken]."[9]

The D.C. Circuit also held that plaintiffs had standing because even if there was no compensation available for actual identity theft, the plaintiffs could be compensated by CareFirst for their costs, such as "the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, [the] cost of conducting a damage assessment, [and] mitigation costs."[10]

In its petition for *certiorari*, CareFirst argued that there is disagreement among the circuit courts, as the Second, Third, Fourth and Eighth Circuits have rejected similar allegations of a risk of future identity theft as a basis for standing. CareFirst also argued that the D.C. Circuit's decision would "open the door to a flood of no-injury class actions arising from virtually every data breach."

IMPLICATIONS

The Supreme Court's decision not to review the *CareFirst* opinion means that plaintiffs will have an easier time in the D.C. Circuit, if not elsewhere, establishing standing in the rising incidence of putative class action litigation due to data breaches. The D.C. Circuit's decision suggests that certain types of personal information have inherent value and, when that information is exposed in a data breach, the individual will have a cognizable injury. Putative class action plaintiffs can be expected to argue that *CareFirst* signifies that standing exists wherever certain sensitive personal information, including credit card or social

security numbers, is exposed in a data breach. In light of this, it is particularly important that upon learning of a data breach, companies immediately notify their insurer, and conduct an investigation that is intended to be protected by privilege with a view to the litigation claims that are likely to arise.

In addition, to the extent that other circuits have rejected similar standing claims by data breach plaintiffs, the *CareFirst* decision may lead plaintiffs to favor the D.C. Circuit in filing future data breach class actions. Companies should be aware that, in appropriate circumstances, they may have personal jurisdiction defenses to such actions.

* * *

ENDNOTES

[1] *See Attias* v. *CareFirst, Inc.*, 199 F. Supp. 3d 193, 201 (D.D.C. 2016).

[2] *See id.*

[3] *Attias* v. *Carefirst, Inc.*, 865 F.3d 620, 625-29 (D.C. Cir. 2017).

[4] *Spokeo, Inc.* v. *Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 560 (1992)).

[5] *Attias*, 865 F.3d at 625-29.

[6] *Id.* at 628-29 (quoting *Remijas* v. *Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015)).

[7] *Id.* at 628-29.

[8] *Id.*

[9] *Id.* at 629.

[10] *Id.*

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Mark F. Rosenberg	+1-212-558-3647	rosenbergm@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com