Simpson Thacher

Memorandum

D.C. Circuit Supports Standing in Data Breach Class-Action Suit, Citing Substantial Risk of Future Identity Theft

August 7, 2017

On August 1, 2017, the U.S. Court of Appeals for the District of Columbia Circuit reversed the dismissal of a putative class action brought after health insurer CareFirst, Inc. suffered a cyberattack. The D.C. Circuit determined that the plaintiffs had standing to sue, because they had plausibly alleged a substantial risk of future identity theft due to the data breach.[1] The decision in *Attias, et al., v. CareFirst, Inc.* puts the D.C. Circuit in line with the Sixth and Seventh Circuits in upholding standing for plaintiffs claiming injury in a data breach case, but at odds with the Second and Fourth Circuit on the issue.

Case Lessons

The holding deepens a split between circuits on whether plaintiffs have standing to bring claims resulting from a data breach. The various decisions have turned on what types of data were accessed and how many customers actually suffered identity theft (or spent money to prevent it) thereafter.[2] *CareFirst* also furthers the possibility that plaintiffs will forum shop and file data breach class actions in favorable jurisdictions.

---

1 *Attias, et al., v. CareFirst, Inc.*, No. 16-7108, 2017 WL 3254941 (D.C. Cir. Aug. 1, 2017), rev'g *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193 (D.D.C. 2016).

2 Compare *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015) (finding standing with 9,200 instances of identity theft after breach affecting 350,000 accounts), *Galaria v. Nationwide Mut. Ins.*, 663 Fed. Appx. 384 (6th Cir. 2016) (finding standing after data breach affecting 1.1 million people without any allegations of actual fraud or identity theft) and *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016) (finding standing for two plaintiffs based on an increased risk of fraudulent charges and money spent on fraud prevention) with *Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116 (2d Cir. May 2, 2017) (dismissing a putative class action brought by a single plaintiff who did not allege any fraudulent charges after minimal customer data were stolen), *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (dismissing a putative class action where there was no actual or attempted misuse of personal information and no indication that personal information had been targeted), *In re Sci. Applications Int'l Corp. ("SAIC")*, 45 F. Supp. 3d 14 (D.D.C. 2014) (two identity thefts out of 4.7 million accounts potentially accessed) and *Antman v. Uber Techs., Inc.*, No. 3:15–cv–01175, 2015 WL 6123054, at *11 (N.D.Cal. Oct. 19, 2015) (no social security or credit card numbers stolen).

Companies should welcome that the district court rejected all but one of the plaintiffs' claims of injury resulting from the breach – (i) overpayment for CareFirst's services, if some of their payment was allocated to the company's cybersecurity efforts; (ii) loss of value in their personal data; and (iii) violation of state consumer protection statutes.[3] The district court recognized – and the D.C. Circuit upheld – plaintiffs' theory of harm based only on their purchase of credit monitoring services to prevent identity theft.

Case Summary

In June 2014, an unknown intruder breached 22 CareFirst computers and reached a database containing the (allegedly unencrypted) personal data of 1.1 million policyholders. CareFirst did not discover the breach until April 2015 and notified its customers a month later. Shortly after the announcement, seven CareFirst customers brought a putative class action, invoking diversity jurisdiction under the U.S. Class Action Fairness Act, 28 U.S.C. § 1332(d), and raising 11 state-law causes of action, including breach of contract, negligence, and violation of consumer-protection statutes.

The complaint alleged unauthorized access to customer names, addresses, subscriber ID numbers, and (this issue was disputed) social security numbers, and that two plaintiffs were already missing their tax refund checks. The plaintiffs sought to certify a class consisting of all CareFirst customers residing in the District of Columbia, Maryland, and Virginia whose personal information had been hacked. CareFirst moved to dismiss for lack of Article III standing and, in the alternative, for failure to state a claim. The district court agreed that the plaintiffs lacked standing, holding that they had alleged neither a present injury nor a high enough likelihood of future injury from the incident.[4] As for the plaintiffs missing their tax refund checks, the district court held that this harm was not "fairly traceable" to any action by CareFirst, because the complaint did not allege that these plaintiffs' social security numbers were stolen.

On appeal, the D.C. Circuit reversed, finding that the district court gave the complaint an unduly narrow reading and that the plaintiffs had cleared the low bar to establish standing at the pleading stage. The D.C. Circuit held that the plaintiffs had Article III standing under *Clapper v. Amnesty Int'l,*[5] based on a substantial risk of future harm stemming from the data breach.

---

3 The Second Circuit rejected similar theories of harm in *Michaels*. 2017 WL 1556116, at *2.

4 Another CareFirst putative class action was brought in the District of Maryland by different plaintiffs who alleged a similar theory. The Maryland district court reached the same conclusion as the D.C. district court and dismissed the case on standing grounds. *See Chambliss v. Carefirst, Inc,* 189 F. Supp. 3d 564 (D. Md. 2016), appeal dismissed (Aug. 31, 2016).

5 133 S. Ct. 1138 (2013). In *Clapper*, the Court held that a data privacy injury must be "concrete and particularized" for the plaintiff to have standing. Later, in the 2016 case *Spokeo v. Robins*, 136 S. Ct. 1540 (2016), the Court clarified that a technical violation of a statute due to a data breach is not necessarily a sufficient, "concrete" harm to confer standing, if the plaintiff does not suffer actual injury or "the risk of real harm."

The Court indicated that it was plausible to infer that the CareFirst hacker had the intent and ability to commit identity theft – "Why else would hackers break into a . . . database?" *Attias*, 2017 WL 3254941 at *6. The Court also stated that CareFirst need not be the most immediate cause (or even proximate cause) of the plaintiffs' injuries to support their claim, if such injuries were "fairly traceable" to CareFirst. The Court further held that the plaintiffs had sufficiently alleged theft of social security numbers in their complaint.

Finally, the Court noted that the plaintiffs had alleged injuries capable of judicial redress; namely that they incurred costs (i) responding to the data breach; (ii) acquiring identity theft protection and monitoring; and (iii) for damage assessment and mitigation.[6]

[6] The D.C. Circuit noted – but deemed unnecessary to address – that two plaintiffs had suffered an actual identity theft because their anticipated tax refund was now missing. The Court also acknowledged but did not address whether CareFirst's alleged violation of state consumer protection law was a distinct injury in fact. *Id.* at *4, n.2.

For any questions relating to liability for data breaches, please contact one of the following members of the Firm.

NEW YORK CITY

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Joseph M. McLaughlin
+1-212-455-3242
jmclaughlin@stblaw.com

Yafit Cohn
+1-212-455-3815
yafit.cohn@stblaw.com

LOS ANGELES

Deborah L. Stein
+1-310-407-7525
dstein@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

Simpson Thacher Worldwide

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
25th Floor, West Tower
Mirae Asset Center 1
26 Eulji-ro 5-Gil, Jung-Gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000