ALERT MEMORANDUM

D.C. Court Rules That Hacking Victims Can Pursue Data Breach Claims Without Showing Actual Loss

August 7, 2017

On August 1, 2017, the United States Court of Appeals for the D.C. Circuit held that policyholders of the health insurer CareFirst had standing to sue the company after their information was compromised during a cyberattack.[1] Wading into a vigorously contested area between plaintiffs and companies that have suffered data breaches, the court held that the policyholders' elevated *risk* of identity theft and medical fraud was a sufficient injury to bring suit—even without any evidence that plaintiffs had *actually* suffered such harm. In so holding, the D.C. Circuit came down on one side of a circuit split, which may ultimately need to be resolved by the Supreme Court.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Jonathan Kolodner
+1212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

WASHINGTON
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1801
T: +1 202 974 1500
F: +1 202 974 1999

Michael Krimminger
+1 202 974 1720
mkrimminger@cgsh.com

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

[1] *Attias v. Carefirst, Inc.*, --- F.3d ---, 2017 WL 3254941 (D.C. Cir. Aug. 1, 2017).

Background

In June 2014, an unknown intruder breached 22 CareFirst computers and accessed a database containing customers' personal information. CareFirst disclosed the breach in May 2015 and, as has become commonplace following such cyberattacks, a group of plaintiffs promptly brought a putative class action in federal district court. The plaintiffs alleged that CareFirst had failed to properly encrypt and protect their personal data, in violation of its customer agreements and various state laws, including consumer-protection statutes. In order to establish their standing to bring suit, as required by Article III of the U.S. Constitution, plaintiffs alleged that they had suffered an increased risk of identity theft as a result of the data breach.

CareFirst moved to dismiss on the grounds that the alleged injury was too speculative to establish an "concrete injury"—beyond an impermissibly "attenuated chain of possibilities"—as required under the Supreme Court's most recent standing decisions.[2] 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. The plaintiffs appealed the lower court's dismissal of the case to the D.C. Circuit.

The D.C. Circuit's Decision And The Circuit Split

The D.C. Circuit reversed the district court's decision and reinstituted the plaintiffs' claims. The court held that the policyholders had "cleared the low bar to establish their standing at the pleading stage" by asserting that there was a substantial risk that their stolen personal information could be used "for ill"—identity theft or medical harm—even though it had yet to be misused. It also ruled that the alleged injury was sufficiently concrete since it was "at the very least . . . plausible" to infer that the cyber intruder had both the intent and ability to use the stolen data for illicit purposes. In so holding, the D.C. Circuit cited a recent Seventh Circuit decision, which had held that customers of Neiman Marcus had standing on the same grounds following a data breach at the luxury retail company.[3]

In addition to the D.C. and Seventh Circuits, at least three other circuits have also held that exposure of consumers' data to *potential* identity theft is sufficient to establish standing. The Sixth Circuit found policyholders could sue on such grounds following a breach at Nationwide Mutual Insurance, the Third Circuit held the same in litigation over a breach at Horizon Healthcare, and the Eleventh Circuit also so held in the context of a breach of Florida health services provider.[4]

These decisions stand in contrast to recent decisions in two other circuits.[5] Earlier this year, the Second Circuit held that a Michaels Stores customer lacked standing to pursue data breach claims because she had not incurred any actual charges on her card or any other concrete injuries. Similarly, the Fourth Circuit held a few months earlier that two classes of military veterans who sued over personal data compromised in two thefts from a VA hospital in South Carolina lacked standing because plaintiffs had failed to point to any evidence that their data had been misused or actually stolen.

Takeaways

While the D.C. Circuit's decision in *CareFirst* aligns it with the majority of courts that have addressed standing in the context of data breach claims, as

[2] *Spokeo, Inc. v. Robins*, --- U.S. ---, 136 S.Ct. 1540, 194 L.Ed.2d 635 (2016); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S.Ct. 1138 (2013).

[3] *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015).

[4] *See Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 WL 4728027, at *1, *3 (6th Cir. Sept. 12, 2016); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012); *In re: Horizon Healthcare Services Inc. Data Breach Litigation*, No. 15-2309, --- F.3d ---, 2017 WL 242554 (3d Cir. Jan. 20, 2017).

[5] *See Whalen v. Michaels Stores, Inc.*, --- F.3d ---, 2017 WL 1556116 (2d Cir. May 2, 2017); *Beck v. McDonald*, 848 F.3d 262, 268 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, No. 16-1328, 2017 WL 1740442 (U.S. June 26, 2017).

described above, there are at least two circuit decisions that are in conflict with the majority position. Ultimately, given these differing outcomes in the Courts of Appeals, the Supreme Court may choose to address the split and have the final word on the issue.

Until then, there will likely be continued litigation over the issue, with parties disputing whether the facts of a particular breach make it plausible that plaintiffs will be victims of identity theft or other fraud. This will likely turn on the types of data compromised, the relationship between the victims of the breach and the data custodian (including any relevant contractual relationship or state laws governing the relationship), and what is known about the source of the breach, if anything. With cyberattacks becoming a daily occurrence, a company's incident response team should keep in mind that the factual investigation will inevitably impact any litigation that may be just around the corner.

…

CLEARY GOTTLIEB