MURTHA CULLINA

NEWS ALERT

PRIVACY & CYBERSECURITY

Can't This Just Be Over? Standing In Cybersecurity Claims

By Michael J. Donnelly and Brad Davis* | January 22, 2018

In August, the United States Court of Appeals for the DC Circuit revived a class action lawsuit, holding that the threat of harm from a data breach is enough to satisfy the "injury in fact" standing requirement. *Attias v. Carefirst, Inc.*, 865 F.3d 620 (DC Cir. 2017). The defendant, a group of health care insurers, filed a Petition for Writ of Certiorari to the United States Supreme Court on October 30 of last year. While the Supreme Court is deciding whether to grant the pending Petition, it is worthwhile to briefly review the standing question in the context of protecting your business from liability.

The standing requirement serves to ensure that courts only address actual controversies brought by parties with a personal stake in the outcome by requiring that a plaintiff show that it has suffered an injury in fact which is concrete and particular, was fairly traceable to the actions at issue and can be redressed by the courts. Increasingly, the plaintiffs bar has responded to incidents of data breach by bringing class action lawsuits based on a number of state law claims and claiming that an increased threat of identity theft constitutes an injury-in-fact.

Courts have split on the issue of whether the threat of harm from a data breach is sufficient to impart standing. The question turns on whether the allegations support a claim that the threatened future harm is "certainly impending" or poses a "substantial risk" of occurring. When the reviewing court finds that the risk is not substantial, then it follows that the claim is speculative and should be dismissed.

In fact, this is what the District Court in *Attias* did, finding that the plaintiffs had not suggested or shown how the hackers could steal their identities without access to social security or credit card numbers. However, the DC Circuit Court of Appeals reversed the District Court's decision, finding that the complaint had actually alleged that social security numbers and credit card information had been compromised. Moreover, the DC Circuit also found that the breach had exposed the plaintiffs to a risk of medical identity fraud whereby someone impersonates a victim and obtains medical services in their name. Such actions could potentially lead to the depletion of the victim's insurance or the receipt of improper medical care as a result of inaccurate medical records.

The Court of Appeals also addressed the causation requirement. CareFirst had argued that because the hackers were unaffiliated with the company, that the claimed injuries would therefore not be fairly traceable to it. The court disagreed, remarking that the causation

Dena M. Castricone, Chair
203.772.7767
dcastricone@murthalaw.com

Burt Cohen, Vice Chair
203.772.7714
bcohen@murthalaw.com

Michael P. Connolly
617.457.4078
mconnolly@murthalaw.com

Michael J. Donnelly
860.240.6058
mdonnelly@murthalaw.com

Melissa A. Federico
860.240.6042
mfederico@murthalaw.com

Daniel J. Kagan
203.772.7726
dkagan@murthalaw.com

Rachel Snow Kindseth
203.772.7774
rkindseth@murthalaw.com

Paul E. Knag
203.653.5407
pknag@murthalaw.com

Bruce L. McDermott
203.772.7787
bmcdermott@murthalaw.com

James F. Radke
617.457.4130
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
203.772.7782
ssobkowiak@murthalaw.com

Ryan M. Suerth
860.240.6157
rsuerth@murthalaw.com

Suzanne Brown Walsh
860.240.6041
swalsh@murthalaw.com

Edward B. Whittemore
860.240.6075
ewhittemore@murthalaw.com

Kristen L. Zaehringer
203.653.5406
kzaehringer@murthalaw.com

requirement does not require that the defendant be the most immediate cause of the claimed injuries. The court found that, at the preliminary stages of the case, a claim that CareFirst had failed to properly secure the data is sufficient.

If the Supreme Court exercises its discretion and grants CareFirst's Petition for Writ of Certiorari, it will likely create a clearer blueprint for analyzing standing issues related to incidents of data breach. However, in the meantime, the practical effect of the caselaw on standing is that any business that suffers a breach where medical, social security, or credit card information is involved, may be faced with a class action lawsuit that likely will survive early legal challenges. Although the plaintiffs must prove the extent of their injuries in order to establish damages at some later point in the suit, the mere fact that there has been a theft of the information is enough to permit plaintiffs to get into court and create expensive litigation for businesses.

WHAT CAN YOUR BUSINESS DO?

(1) Collect only the information that is necessary to operate your business;

(2) Consider outsourcing payment functions to a vendor so that no payment information is maintained;

(3) Provide adequate security protections based on a risk assessment; and

(4) Obtain cyber risk coverage that will cover litigation costs.

If you have any questions regarding privacy and cybersecurity issues, please contact Michael J. Donnelly at 860.240.6058 or mdonnelly@murthalaw.com or Dena M. Castricone at 203.772.7767 or dcastricone@murthalaw.com.

**Brad Davis is a Legal Intern at Murtha Cullina LLP.*