Court Expands Standing for Plaintiffs to Pursue Data Breach Claims

On August 1, 2017, the D.C. Circuit handed down its decision in the data breach class action *Attias v. CareFirst*. In doing so, it became the latest federal appellate court to recognize that individual victims of a breach have standing to bring claims based on the risk of future harm that they may suffer. Importantly, in reaching this conclusion, the three-judge panel unanimously emphasized that the breach—which compromised plaintiffs' social security and credit card numbers—could create a "substantial risk" of injury, thereby determining that the plaintiffs could proceed with their case beyond the pleading stage. By overturning a lower court decision to dismiss the case and allowing the plaintiffs to proceed with their claims, *CareFirst* builds on multi-circuit precedent establishing the viability of civil suits stemming from data breaches. Companies should be aware of this precedent and prepare themselves as a growing number of courts demonstrate a willingness to open the door to civil liability following a cyber incident.

Carefirst and Injuries Resulting from Data Breaches

The *Carefirst* case emanates from a 2014 cyberattack whereby hackers infiltrated 22 of health insurance carrier Carefirst BlueCross BlueShield's computers. As a result of the attack, more than a million policyholders had their data compromised. The compromised data included names, birth dates, email addresses, policy identification numbers, social security numbers and credit card numbers. Subsequently, a number of victims filed suit against Carefirst and sought to certify a class of all affected individuals in the District of Columbia, Maryland, and Virginia.

The district court dismissed the plaintiffs' suit on standing grounds. After erroneously noting that the complaint did not allege that social security and credit card numbers were among the compromised data, the court held that any injury resulting from the breach was too speculative. Specifically, it found that the plaintiffs did not demonstrate an "injury in fact"—that their injury was concrete, particularized and "actual or imminent"—rather than merely possible.

On appeal, the D.C. Circuit reversed the district court, noting at the outset that the plaintiffs had in fact alleged that the compromised information included social security and credit card numbers. More importantly, given the nature of the compromised information, the appellate court held that there was a "substantial risk" that injury would occur as a result of the breach, and as such, the suit could proceed. In overturning the district court, the appellate court emphasized that alleged injuries need only be plausible to meet standing requirements. The court reasoned that identity thieves could use the stolen data "to open new financial accounts, incur charges in another person's name and commit various other financial misdeeds." Additionally, the appellate court found that the plaintiffs alleged a substantial risk of "medical identity theft" because the compromised information included policy identification numbers in conjunction with other personally identifying information. In the wrong hands, this information could be used in ways that would cause victims to "receive improper care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs."

The court distinguished the facts in this case with those in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). Whereas *Clapper* involved harm that would only arise if "independent actors . . . exercised their independent judgment in a specific way," the hackers in *Carefirst* had already accessed sensitive information. Based on this access, "it is plausible . . . to infer that this party has both the intent and the ability to use the data for ill." Put differently, no "long sequence of uncertain contingencies . . . has to occur before plaintiffs in this will suffer any harm; a substantial risk exists already, simply by virtue of the hack and the nature of the data." While limited to

the facts of the case, this reasoning could be used to support standing in many other contexts involving hacks, breaches, and cyberattacks.

Looking Ahead

The D.C. Circuit is not the first court to conclude that the allegations of future harm are sufficient to support a civil case following a data breach. The Third, Seventh, and Ninth circuits have all permitted suits to proceed in which the alleged injury stems from stolen personal information. Taken together, these decisions have expanded the ability of plaintiffs to pursue claims against companies for breach of their sensitive information. As a result, companies that collect, store, and process sensitive information now face a greater risk of liability. Moreover, the cost of defending against these claims may become exponentially more expensive, given the increased likelihood that such a claim will survive a motion to dismiss.

In addition to being aware of the increasing liability resulting from a data breach, companies can draw several lessons from *Carefirst*. First, courts are increasingly willing to expand their views of harm to protect consumers against the new and changing threats posed by modern technology. The shift to a digital-based economy has increased the risk of identity theft and the extent of harm posed to consumers. Vast quantities of sensitive consumer data are being collected and can be transmitted across borders in an instant. Expanding opportunities for punitive liability provides consumers with relief and increases accountability of companies for the data that they collect. Second, courts are more likely to support civil liability when especially sensitive information is implicated. The fact that social security, credit card and policy identification numbers were among the compromised data was significant in the court's analysis of the potential harm the plaintiffs may suffer.

It is more important than ever that companies carefully consider the strength of their information governance strategy—how they store and protect sensitive information and how they prepare for, respond to, and mitigate a cyber incident. Such incidents already have severe consequences, and with the current trend toward increased liability, it is in every company's interest to avoid being the next headline.

Tracy L. Lechner
Shareholder
tlechner@bhfs.com
303.223.1274

Jonathan C. Sandler
Shareholder
jsandler@bhfs.com
310.564.8672

Ian V. O'Neill
Shareholder
ioneill@bhfs.com
303.223.1210

Esteban M. Morin
Associate
emorin@bhfs.com
303.223.1275