alert Cybersecurity and Privacy Practice

Saul Ewing LLP

AUGUST 2017

In Data Breach Lawsuit, Mere Risk of Identity Theft is Enough to Stand On

Author:
Malia K. Rogers

SUMMARY

As the frequency of data breach incidents increases at a record pace, courts are becoming less reluctant to open the floodgates and allow consumers to bring data breach lawsuits. In its recent *Attias v. CareFirst, Inc.* opinion [http://bit.ly/2wM9CD9], the D.C. Circuit held that the plaintiffs had standing to bring a lawsuit by alleging they suffered a mere risk of future identity fraud resulting from a breach—rather than requiring that they suffered actual identity fraud—joining similar decisions by the Third, Sixth, Seventh, and Eleventh Circuits. The Second and Fourth Circuits have found the opposite, making this issue ripe for the Supreme Court's review. But until the Supreme Court tackles the issue, the majority's relaxed view of standing will result in an increased risk of liability for organizations that collect and store data, underscoring the importance of proactively implementing cybersecurity safeguards so that organizations are not found to be negligent should a data breach matter arise.

The *Attias v. CareFirst* Decision

In June 2014, an unknown hacker breached health insurer CareFirst's computer system, compromising the personal information of some 1.1 million policyholders. CareFirst discovered the breach 10 months later and notified its customers the following month.

Soon after, seven CareFirst customers filed a class action on behalf of all D.C., Maryland, and Virginia customers whose personal information had been hacked. The plaintiffs alleged an increased risk of *future* identity theft as a result of CareFirst's negligence in failing to properly encrypt some of the personal data it collected and stored.

The United States District Court for the District of Columbia dismissed the class action for lack of standing, finding the risk of identity theft to be too speculative to constitute an "injury-in-fact." Specifically, the district court did not read the complaint to allege any actual theft of social security or credit card numbers, and concluded that the plaintiffs failed to show how the hackers could steal their identities.

On appeal, the D.C. Circuit reversed, finding that the threat of future harm as a result of compromised personal information is a real, concrete harm sufficient for standing under Article III. The court reasoned "[w]hy 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."

The D.C. Circuit recognized that a substantial risk of harm exists simply by virtue of the hack and the nature of the data, regardless of whether social security or credit card data was exposed to the hacker. The combination of the other personal information stolen, including names, birthdates, email addresses, and subscriber identification numbers, alone was determined to present a substantial risk of identity fraud.

Takeaways

The D.C. Circuit's decision tracks the holdings of a majority of the circuit courts, which have found standing based on the imminent threat of identity fraud, rather than requiring allegations of actual harm. While the D.C. Circuit noted that "the burden [on the plaintiffs] grows as the litigation progresses," more and more data breach lawsuits will survive the motion to dismiss stage rather than being quickly dismissed based on lack of standing. Even if data breach claimants are not ultimately successful, organizations will be exposed to increased litigation costs and subject to a greater risk of liability (which in turn will increase settlement costs).

As the law continues to evolve in this area and courts come to appreciate the serious consequences of data breaches, organizations that collect and store personal information face increased exposure. Organizations should review their cybersecurity protocols and safeguards so that the risk of any negligence claims are minimized should a data breach matter arise.

Saul Ewing's Cybersecurity and Privacy Practice is able to assist organizations in assessing their cybersecurity risks and taking proactive steps to mitigate and reduce those risks. For more information on these matters, please contact the author or the attorney at the firm with whom you are regularly in contact.

This Alert was written by Malia K. Rogers, a member of the firm's Cybersecurity and Privacy Practice. Malia can be reached at 215.972.7766 or mrogers@saul.com. This publication has been prepared by the Cybersecurity and Privacy Practice for information purposes only.