Data Breach Class Action Reinstated - Despite No Actual Identity Theft

August 2, 2017

Must plaintiffs allege actual identity theft from a data breach to avoid dismissal of their class action lawsuit? No, according to yesterday's opinion from a three-judge panel of the United States Court of Appeals for the District of Columbia Circuit.

In *Attias v. CareFirst, Inc.*, Case No. 16-7108 (DC Cir. Aug. 1, 2017), the DC Circuit reinstated a dismissed class action against a health insurer for its alleged negligence in permitting a 2014 data breach that exposed the personal information of approximately 1.1 million customers. The district court had found the alleged damages too speculative because the customers had not suffered actual identity theft, but merely faced an increased risk. The DC Circuit reversed, holding that the complaint plausibly alleged a substantial risk of "imminent" identity theft that was "fairly traceable" to defendant.

The *Attias* Court was willing to infer damages to support the class action for plaintiffs whose identities remained intact: "Why 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." Id. (quoting *Remijas* v. *Neiman Marcus Grp*., 794 F.3d 688, 693 (7th Cir. 2015)). The Court rejected a narrower reading of two recent Supreme Court decisions on the "injury in fact" standing requirement, *Spokeo v. Robins* (2016) and *Clapper v. Amnesty International USA* (2013).

The net effect of this opinion is more risk for business. In its *amicus* brief, the US Chamber of Commerce argued that such no-injury lawsuits based on anxiety about speculative future harm impose significant and unjustified costs on businesses. Rather than obtain a dismissal at the outset of expensive class action litigation, companies will be forced to engage in discovery and seek summary judgment on the facts established.

In the end, this opinion is another reminder to companies that they must inventory and take reasonable measures to protect personally identifiable information (PII) and protected health information (PHI) that they own or maintain. For example, the *Attias* complaint alleged that CareFirst failed to properly encrypt some of the data entrusted to its care. Encrypted data is not only less susceptible to a breach, it does not count as

PII so as to trigger breach notification under many state statutes. A working Information Security Plan helps a company determine how to best identify and prioritize its data, prevent improper access to its systems and mitigate the risks of a breach.

The opinion may be found here.

If you have questions about this alert, please contact your Lathrop Gage attorney or either of the attorney listed above.