MINTZ

D.C. Circuit Holds Cyber-Theft of Customers' Medical Identifying Information Created Sufficient Increased Risk of Harm to Establish Standing

September 01, 2017 | Blog | By **Patrick E. McDonough**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Earlier this month, an appellate panel of the federal DC Circuit unanimously held that individuals affected by a healthcare insurer's data breach in 2014 could pursue claims against the insurer stemming from the cyberattack. In the process, the panel deepened a circuit split on the question of whether data breach victims have standing to pursue claims based solely on exposure of their sensitive personal information, while also adding significant risk of cyber-liability for companies that collect and store medical records of individuals.

In ***Attias v. CareFirst, Inc.***, the plaintiffs asserted claims on behalf of a purported class of one million customers of CareFirst, Inc. ("CareFirst"), a healthcare insurer in the Washington, DC metro area. In the 2014 cyberattack, hackers penetrated 22 computers and compromised the identifying health data of one million customers, including customer names, addresses, email addresses, subscriber ID numbers, and Social Security numbers. The plaintiffs did not allege that they had suffered any direct financial injury as a result of their identifying health data being exposed, but did allege they suffered an "increased risk of identity theft" as a result of CareFirst's alleged negligent conduct. The district court granted CareFirst's motion to dismiss, which asserted that the plaintiffs lacked standing to bring their alleged claims because they had not asserted either a present injury arising from the data breach or a "high enough likelihood of future injury."

On appeal, the DC Circuit held that the district court's view of standing was too narrow under the standard established by the Supreme Court in t ***Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016)**. *Spokeo* held that, to satisfy the standing requirement of Article III of the Constitution, a plaintiff must allege and prove he or she suffered an "injury in fact" that is "fairly traceable" to a defendant's conduct, and that said injury is "likely to be redressed" by the relief sought. As applied in data breach cases, that standard obligates a plaintiff to show that his or her injury is "***actual*** or ***imminent***" rather than speculative. ***See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013)**. The district court had determined the plaintiffs' alleged "increased risk of identity theft" as a result of the breach was ***not*** sufficiently "actual or imminent" and thus could not meet the standing requirements. According to the district court, there was no actual or imminent exposure to a heightened risk of identity theft as a result of the 2014 cyberattack, or sufficient risk of an imminent future injury arising thereof. Because the plaintiffs' stolen information had not yet been used to harm them, the district court found they could not demonstrate "actual or imminent" harm at the pleading stage.

The DC Circuit disagreed, holding that although no injury had in fact occurred, it was sufficient that plaintiffs established either (1) their threatened injury arising from the data breach was impending with certainty ***or*** (2) CareFirst's conduct created a substantial risk that injury could occur as a result of the breach. According to the DC Circuit, a plaintiff may establish this latter prong – that a "substantial risk" that injury could occur – by showing the defendant's conduct created a "significant risk" or "substantial probability" of injury.

Under the DC Circuit's analysis, a plaintiff cannot establish that there is a substantial risk injury could occur when the unrealized injury is too attenuated from the defendant's alleged conduct. In data breach actions such as this one, whether the defendants' conduct creates a sufficient increased risk of harm depends upon the type of identifying data stolen. Because the hackers stole CareFirst customers' medical identifying information (including names, addresses, Social Security numbers and subscriber ID numbers), it was plausible that persons could use this information to commit identity theft. The victims of the CareFirst breach could plausibly allege that the "nature of the hack" and the "nature of the data" immediately created a substantial risk that they would suffer an injury from the theft, even if one had not yet occurred. Put another way, there was "no long sequence of uncertain contingencies" that needed to

occur in order for the CareFirst victims to suffer harm resulting from the data breach. Given the nature of the medical records that were stolen as a result of the data breach, the DC Circuit noted it could presume that the hackers had the "intent and ability to use the [medical records] for ill."

The DC Circuit's opinion in *CareFirst* shows that the risk of liability for companies suffering data breaches will likely depend on the type of customer information they collect and store. The DC Circuit's holding rested on the particular mix of customer information stolen and the industry in which CareFirst operated (the healthcare industry). For example, in cases involving theft of payment card data, the risk of harm to consumers is non-existent, given that payment card customers do not pay for fraudulent transactions and no identity theft can result from only a credit card number. Medical records, however, contain sensitive personal information – including dates of birth and Social Security numbers – that serve as a starter kit for identity theft. The DC Circuit indicated that plaintiffs likely have standing to sue in cases where the data stolen includes social security numbers or this specific medical identifying information. Otherwise, it would be possible to distinguish *CareFirst* from cases arising from payment card data breaches. This clear distinction in the case law now imposes a heightened risk on companies that create and store medical records of their customers, as theft of this data creates a substantial risk of identity theft that exposes these companies to significant potential liability in the result of a data breach.

Recent case law among the circuits shows a distinct split in data breach actions concerning the issue of whether an increased risk of identity theft constitutes sufficient "actual or imminent" injury for Article III standing purposes. The DC Circuit's opinion in *CareFirst* joins the Sixth Circuit's opinion in ***Galaria v. Nationwide Mut. Ins. Co.*** the Seventh Circuit in ***Remijias v. Neiman Marcus Group LLC***, and the Third Circuit in ***In re Horizon Healthcare Services Data Breach Litig.*** in holding that data breach litigants have standing to sue in certain circumstances even where they cannot allege they have suffered an actual injury in fact as a result of the breach. In contrast, the Second Circuit in *Whalen v. Michaels Stores* and the Fourth Circuit in *Beck v. McDonald* have both held that an increased risk of identity theft is not sufficient for a data breach litigant to establish Article III standing. This circuit split of course increases the likelihood that the Supreme Court will take up a similar case in the near future and resolve this conflict. Until then, the circuit split increases the chances that data breach litigants will forum shop and bring litigation in friendly jurisdictions where their claims are likely to survive at least the motion to dismiss stage.

Until this circuit split is resolved, companies that collect sensitive personal information – especially health care providers, insurers and other entities – should ensure that they have in place effective privacy programs that protect this data and reduce the probability of cyber theft. Because medical records and health insurance information likely creates a substantial risk of identity theft when stolen, health insurance companies, healthcare providers, and other companies that possess and store these types of data must take extra precautions to ensure this data is protected to the greatest extent possible.

Authors

Patrick E. McDonough, Associate

Patrick is an associate in the litigation practice where he focuses on securities and shareholder litigation, as well as investigations and securities enforcements. He represents clients from early-stage start-ups to publicly-traded companies in numerous industries, including life sciences and biotechnology companies, financial services, consumer products and retail, and clean technology.