HUDSON COOK 25th ANNIVERSARY

Exploring the Standing Challenge in Data Breach Litigation

March 28, 2018 | Michael A. Goodman and Kavitha J. Subramanian

As data breaches become more commonplace, courts have taken different approaches to address when an increased risk of prospective consumer harm is sufficiently concrete to establish standing for purposes of asserting a claim in federal court. Some courts have taken the position that a showing of an increased risk of identity theft, even without evidence of an actual misuse of the consumer's information, is a sufficiently imminent injury to establish standing. However, even in these cases, whether the increased risk of harm is concrete and imminent depends on the type of information stolen.

In *Fero v. Excellus Health Plan, Inc.*, the U.S. District Court for the Western District of New York recently reversed its position regarding the plaintiffs' standing, holding that a data breach resulting in the disclosure of personally identifiable information ("PII") that caused an increased risk of future identity theft was sufficient to give the plaintiffs standing to pursue claims stemming from the breach.

In December 2013, Excellus Health suffered a data breach where the information of millions of individuals, including their names, birthdates, social security numbers and payment information, was stolen. Matthew Fero sued Excellus Health on behalf of himself and a class of similarly situated consumers for common law negligence, breach of contract, and privacy violations arising out of the breach. Excellus Health filed a motion to dismiss for lack of Article III standing. In February 2017, the court partially granted the motion to dismiss as to certain members of the class, finding that certain plaintiffs failed to allege that they suffered any actual misuse of their PII and a risk of future identify theft was not sufficient to establish an injury in fact for Article III standing. The plaintiff class moved for reconsideration of the order. The court granted the motion and reversed its earlier ruling.

The plaintiff class sought reconsideration based on the recent unpublished ruling of the U.S. Court of Appeals for the Second Circuit in *Whalen v. Michaels Stores, Inc.*, where the court indicated that the risk of future identify theft could be sufficiently concrete to confer Article III standing. In *Whalen*, the defendant's data breach compromised the plaintiff's credit card information. After noticing fraudulent charges on her card, the plaintiff cancelled the card and was not liable for any of the charges. The *Whalen* court found that because the plaintiff cancelled the card and no other PII was stolen, she could not allege that she plausibly faced a threat of future fraud. The *Whalen* court reasoned, however, that if the plaintiff had not cancelled her credit card, then the risk of future harm could have constituted an injury in fact. The plaintiff class in *Fero* argued that *Whalen* stands for the proposition that plaintiffs do not need to wait for their identities to be stolen before they can seek legal recourse. Instead, the plaintiff class argued, and the court agreed, that if the risk of future harm can be alleged as a direct and proximate result of the defendant's actions in a data breach, it is sufficient to establish an injury in fact.

The *Fero* court also found persuasive the recent U.S. Court of Appeals for the D.C. Circuit case, *Attias v.*

CareFirst, Inc. The *Attias* court concluded that threatened future identity theft resulting from a data breach that compromised the consumers' names, birthdates, social security numbers and credit card numbers posed a substantial risk of occurring, which was sufficient to establish standing. The court found that the mere existence of the hack and the stealing of sensitive PII about consumers proved there was an intent and ability to use the data for nefarious purposes.

Similarly, in *Fero*, the court reasoned that the type of PII disclosed in the Excellus Health breach could lead to a variety of future fraudulent conduct, which established an injury in fact. The court found that this was also supported by new evidence introduced by the plaintiff class showing that data from the Excellus Health breach was available on the dark web. The court found that because the information was on the dark web, it was clear that the attacker intended to use the consumers' PII to commit identity theft. Accordingly, the court found that the risk of harm resulting from the theft of PII such as a social security number and financial information was sufficiently concrete and imminent to establish standing.

The decision in *Fero* is not necessarily indicative of how the Second Circuit may eventually rule on the issue of standing. Currently, the Third and Fourth Circuit Courts of Appeal have found a future risk of identity theft to be too speculative to establish standing, specifically when there is no proof that any of the information stolen in the data breach was actually misused. Conversely, the D.C. Circuit and the Sixth, Seventh, and Ninth Circuit Courts have found that the risk of future harm is sufficient to establish standing because the theft of PII indicated that the threat of misuse was imminent. The U.S. Supreme Court recently denied certiorari in *CareFirst v. Attias*, allowing the circuit split to persist. It appears that the issue of standing in data breach cases will continue to be an evolving area of law, where the outcome will vary depending on the type of information breached and the consumer's showing of a risk of actual harm.

HUDSON
COOK

Celebrating its 25th anniversary in 2022, Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

www.hudsoncook.com