KILPATRICK TOWNSEND

February 13, 2019

Is standing overrated? Data breach defendants who lose standing battles end up winning dismissal on the merits.

by James F. Bogan III

Takeaway: In the wake of *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), defendants in data breach class actions regularly move to dismiss on standing grounds, arguing the complaint's allegations do not plausibly allege an injury-in-fact fairly traceable to the defendant's conduct. Prevailing on the standing issues, however, means the district court does not have jurisdiction to resolve the merits of the dispute – it can only enter a procedural dismissal without prejudice. Moreover, where a standing challenge succeeds in federal court, the same claims could potentially be re-filed in state court and not removed to federal court (because the defendant already succeeded in showing the absence of federal jurisdiction). As two recent data breach rulings illustrate, rejections of standing challenges may be blessings in disguise, because the defendants went on to obtain comprehensive or near-comprehensive victories on the merits for failure to state a claim.

In *Attias v. CareFirst, Inc.*, No. 15-cv-00882(CRC), 2019 WL 367984 (D.D.C. Jan. 30, 2019), the district court dismissed most of the claims on the merits after the D.C. Circuit reversed its decision dismissing a data breach class action on standing grounds. The *Attias* case arose out of a data breach at CareFirst, a Washington, D.C.-based healthcare insurer, that compromised the personal data of millions of its policyholders. Various of those policyholders brought putative data breach class actions against CareFirst, seeking civil remedies under both contract and tort-based theories under the laws of the District of Columbia, as well as statutory consumer protection claims under D.C., Maryland, and Virginia law.

All of the class plaintiffs alleged that CareFirst had failed to take reasonable steps to protect their personal information. But most of the alleged injuries did not involve actual misuse of personal information. Rather, the class plaintiffs alleged that they were subject to an increased risk of future identity theft, and that this risk required them to take various precautions, such as paying for credit monitoring services. They also alleged that CareFirst breached its contractual obligations to the plaintiffs because it had failed to provide adequate data security, which, they alleged, was part and parcel of their contractual bargain with CareFirst. And the plaintiffs suffered other alleged harms as well, including emotional distress.

The district court initially dismissed the class plaintiffs' claims for failure to allege Article III standing. *Attias v. CareFirst, Inc*., 199 F. Supp. 3d 193 (D.D.C. 2016). But the D.C. Circuit reversed and remanded, concluding that the plaintiffs had plausibly alleged a substantial risk of identity theft sufficient to satisfy "the light burden of proof the plaintiffs bear at the pleading stage." *Attias*, 2019 WL 367984, at *3 (quoting *Attias v. CareFirst, Inc*.,

865 F.3d 620, 627-28 (D.C. Cir. 2017)).

On remand, CareFirst renewed its Rule 12(b)(6) motion to dismiss the claims on the merits. After confirming that the court had subject matter jurisdiction over the claims under the Class Action Fairness Act, the district court concluded that, "while plaintiffs' alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the 'actual damages' element of nine of their state-law causes of action." *Id.* at *1. The district court further addressed CareFirst's economic loss rule argument, "finding that the parties' non-fiduciary contractual relationship independently forecloses tort liability based on the allegations in the complaint." *Id.*

Ultimately, the district court dismissed all of the putative class plaintiffs' claims other than the claims of two class plaintiffs who alleged they experienced "tax-refund fraud" as a result of the CareFirst data breach. And these plaintiffs could pursue only two substantive claims, for breach of contract and violation of the Maryland Consumer Protection Act. *Id.* at *20. These limited categories of actionable theories of injuries may give rise to serious class certification challenges, given the apparent lack of evidence any other member of the putative class suffered actual losses as a result of the data breach.

The data breach defendant similarly obtained a favorable merits ruling after the reversal of a standing dismissal in *In re: SuperValu, Inc., Customer Data Security Breach Litigation,* No. 14-MD-2586 ADM/TNL, 2018 WL 1189327 (D. Minn. Mar. 7, 2018). There, the district court originally dismissed the data breach class action for failure adequately to allege Article III standing. On appeal, the Eighth Circuit largely agreed with the district court, but the appellate court reversed and remanded, based on an "isolated single instance of an unauthorized charge" suffered by class representative David Holmes. *In re Supervalu, Inc*., 870 F.3d 763, 768, 772-774 (8th Cir. 2017).

The Eighth Circuit acknowledged a number of key omissions in Mr. Holmes' allegations, including "that he failed to allege the date he shopped at the affected [SuperValue] store, the amount of the charge, or that the charge was unreimbursed." *Id*. at 773. "While such omissions could be fatal to the complaint under the 'higher hurdles' of Rules 8(a) and 12(b)(6)—a contention that we do not opine on here—standing under Article III presents only a 'threshold inquiry' requiring 'general allegations' of injury, causation, and redressability. We conclude that these attacks on the sufficiency of Holmes' allegations are more properly directed at whether the complaint states a claim, not whether Holmes has alleged standing." *Id*. (citations omitted).

Not surprisingly, SuperValue renewed its motion to dismiss on remand, and the district court dismissed all remaining claims with prejudice. Among other rulings, the district court dismissed the negligence claim because Mr. Holmes did not allege an out-of-pocket loss (he did not allege he paid the fraudulent charge or that any payment was not reimbursed). 2018 WL 1189327, at *11-13. The district court also rejected the negligence claim based on the economic loss rule, finding the plaintiff did not allege personal injury or property

damage. *Id*. at *13-14. And the court further noted that courts had consistently declined to impose a duty in tort under Illinois law to protect personal information. *Id*. at *14. The plaintiff's claim under the Illinois Consumer Fraud and Deceptive Practices Act failed because he failed to allege actual pecuniary loss. *Id*. at *15. And the unjust enrichment claim failed because the plaintiff conceded he had obtained goods of value from SuperValue. *Id*. at *16-17. The district court did not accept the argument that he paid "for a side order of data security and protection." *Id*. at *16.

The *Attias and Supervalu* cases illustrate the high hurdles a defendant must clear to secure a standing-based dismissal of a data breach claim. But they also confirm that losing the standing battle may merely be a prelude to winning the merits war. At a minimum, these cases confirm that every motion to dismiss on standing grounds should also be accompanied by a corresponding motion to dismiss on the merits. And in a data breach case where no class plaintiff alleges an actual monetary loss, class defendants should consider seeking a merits-based dismissal rather than a dismissal without prejudice for lack of standing.