CARLTON FIELDS

Circuit Split on Standing in Data Breach Class Actions Survives Clapper

September 23, 2015

On September 17, the Seventh Circuit Court of Appeals denied a retailer's petition for rehearing en banc of a three-judge panel opinion holding that plaintiffs whose credit card information was stolen in a data breach had standing to sue under Article III of the United States Constitution based on alleged fear of future identity theft. The litigation arose from a cyberattack on luxury retailer Neiman Marcus over the 2013 holiday shopping season in which hackers may have gained access to 350,000 credit and debit cards. Plaintiffs, all of whom made credit or debit card purchases from the retailer during the relevant time period, filed a putative class action lawsuit on behalf of themselves and all other customers whose card information may have been compromised. Neiman Marcus moved to dismiss for lack of standing; the district court granted that motion. On appeal to the Seventh Circuit, a three-judge panel first addressed whether the plaintiffs' two purportedly "imminent" future injuries—"an increased risk of future fraudulent charges" and "a greater susceptibility to identity theft"—satisfied Article III's injury in fact, causation, and redressability requirements. In finding that the plaintiffs' alleged future injuries satisfied Article III, the opinion first considered the injury in fact requirement—starting with the acknowledgment that the Supreme Court's 2013 holding in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), requires that any alleged "future harm" be "certainly

impending" and that "allegations of possible future injury are not sufficient." Taking issue with the lower court and other district courts that dismissed putative data breach class actions for lack of standing under *Clapper*, the Seventh Circuit panel found that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing." The court specifically distinguished the facts of the data breach class action from those in *Clapper*, finding that the plaintiffs here had shown a substantial risk of harm from the data breach because there was no dispute that various customers' card information had been stolen and because "the purpose of [a] hack is, sooner or later, to make fraudulent charges or assume those customers' identities." Indeed, 9,200 of the cards had already incurred fraudulent charges; further, the panel noted that the retailer's offer of free credit monitoring services tacitly acknowledged the likelihood of future unauthorized charges. The court also found that the plaintiffs satisfied Article III's causation and redressability requirements, rejecting Neiman Marcus's causation argument that the plaintiffs' injury was not fairly traceable to its conduct because fraudulent charges could be attributable to data breaches at several other large retailers that occurred at approximately the same time. The opinion stated that such an argument had "no bearing on standing to sue" and was, "at most, a legal theory that Neiman Marcus might later raise as a defense." Further, the court rejected the retailer's argument that the plaintiffs' injury would not be redressed by a judicial opinion because they already were reimbursed for fraudulent charges and the retailer offered to provide all potentially affected customers with a year of free credit monitoring services. The court reasoned that "reimbursement policies vary," debit cards typically receiving less protection than credit cards; hence, "a favorable judicial decision could redress any [future] injuries caused by less than full reimbursement of [future] unauthorized charges." The Seventh Circuit opinion is troubling for businesses, which are also the victims in cyberattacks and had hoped, in the wake of *Clapper*, to receive some judicial relief from putative data breach class actions where the plaintiffs were admittedly offered free credit monitoring and were reimbursed for any fraudulent charges allegedly incurred as a result of the breach. Indeed, the opinion's lenient view of Article III's standing requirement, coupled with a recent circuit opinion rejecting a "heightened" ascertainability requirement, *Mullins v. Direct Digital, LLC*, No. 15-1776, 2015 WL 4546159 (7th Cir. July 28, 2015), may mark the Seventh Circuit as an emerging venue of choice for the plaintiffs' class action bar. However, there may yet be a silver lining for corporate defendants, as the panel remanded the case to the lower court to consider the retailer's pending motion to dismiss for failure to state a claim. *See, e.g.*, *Moyer v. Michaels Stores, Inc.*, No. 14c561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (finding Article III's standing requirement was met in a putative data breach class action notwithstanding *Clapper*, but granting motion to dismiss because the plaintiffs failed to allege actual monetary damages—a required element of their claims—as neither an increased risk of identity theft nor the purchase of credit monitoring services constitute cognizable monetary damages). In denying the retailer's petition for rehearing *en banc*, the Seventh Circuit has confirmed that the circuit split on the issue of standing in data breach class actions survives *Clapper*. Although the Supreme Court in 2012 denied a petition for writ of certiorari to address the question of standing in data breach cases, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), cert. denied, 132 S. Ct. 2395 (2012), it is anticipated that the court may again be asked to resolve the circuit split in the near future. *Remijas v. Neiman Marcus Group,*

LLC, No. 14-3122, 2015 WL 4394814 (7th Cir. July 20, 2015), reh'g denied (Sept. 17, 2015). *Portions of this article previously appeared on Classified: The Class Action Blog and the ABA Section of Litigation's Class Actions & Derivative Suits Newsletter.*

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology