CARLTON FIELDS

Are Data Breach Cases the Next Wave of Class Action Litigation?

November 19, 2014

In the Carlton Fields 2014 Class Action Survey, general counsel and senior legal officers of 326 companies identified data privacy and security as the area of law most likely to give rise to the next wave of class action litigation. Recent developments suggest that they have cause for concern. Historically, the requirement of standing under Article III of the United States Constitution has been a significant obstacle for putative data breach class actions. In 2012, the U.S. Supreme Court denied review to resolve a circuit split on whether a plaintiff in a putative data breach class action has standing where the plaintiff alleges that personal, nonpublic information (including date of birth, Social Security number, and bank account information) was compromised via a data breach, increasing the plaintiff's risk of identity theft and causing the plaintiff to incur costs for credit monitoring. *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3rd Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (2012); Petition for Certiorari, *Reilly v. Ceridian Corp.*, No. 11-1128, 2012 WL 865211 (Mar. 12, 2012). Following that, the Supreme Court decided *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), a case arising outside the class action context in which various human rights and media organizations challenged the constitutionality of a provision of the Foreign Intelligence Surveillance Act authorizing surveillance of communications with persons outside the United States. The plaintiffs asserted that they had standing to challenge the provision because they engaged in sensitive communications with internationals who they believed were targets of surveillance, making the plaintiffs' communications likely to be intercepted by the government. The Second Circuit agreed. In a 5–4 opinion, the Supreme Court reversed, holding that "respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm." Several federal district courts have since dismissed putative data breach class actions for lack of standing. *See, e.g.*, *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, No. 12–347 (JEB), 2014 WL 1858458, at *10 (D.D.C. May 9, 2014); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 464–65 (D.N.J. 2013). Those courts have reasoned that under *Clapper*, the threat of injury must be "certainly impending" to give rise to standing. Yet, after a data breach, victims may not suffer financial harm immediately. Often they find that their identity or financial accounts are compromised months or years after the breach occurred. The Seventh, Ninth, and Eleventh Circuits have yet to address whether *Clapper*

overrules prior circuit precedents finding that standing was met in the context of putative data breach class actions. Within the Seventh Circuit, at least one federal district court has held that *Clapper* overruled Seventh Circuit precedent finding that Article III's standing requirements were satisfied by a would-be data breach class action representative. *See Strautins v. Trustwave Holdings, Inc.*, No. 12–cv–09115, 2014 WL 960816, at *5 (N.D. Ill. Mar. 12, 2014). Another federal district court dismissed putative data breach class action claims under *Clapper* with no discussion of the Seventh Circuit's prior precedent. *See In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *3–6 (N.D. Ill. Sept. 3, 2013). A third federal district court distinguished the Seventh Circuit's prior precedent, finding that the plaintiffs alleged only that their personal, nonpublic information *may have been* stolen, in contrast with the Seventh Circuit's precedent, in which plaintiffs alleged their information *had been* stolen. *Remjas v. Neiman Marcus Grp., LLC*, No. 14vc1735, 2014 WL 4627893, at *2–4 (N.D. Ill. Sept. 16, 2014). Finally, a fourth federal district court found that Article III's standing requirement was met in a putative data breach class action, notwithstanding *Clapper*, in part because *Clapper*'s standing review was "especially rigorous" because the case involved national security and constitutional concerns. *Moyer v. Michaels Stores, Inc.*, No. 14 c 561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014). But that court nonetheless granted the motion to dismiss because the plaintiffs failed to allege actual monetary damages, as neither an increased risk of identity theft nor the purchase of credit monitoring services constitute cognizable monetary damages. Within the Ninth Circuit, federal district courts in California have bucked the trend on standing, finding that putative data breach class action plaintiffs satisfied Article III's requirements as articulated in *Clapper*. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962–63 (S.D. Cal. 2014); *In re Adobe Sys., Inc. Privacy Litig.*, No. 13-CV-05226-LHK, 2014 WL 4379916, at *9 (N.D. Cal. Sept. 4, 2014). Specifically, the *Adobe* court denied the motion to dismiss in part because the plaintiffs have standing based on their increased risk of future harm from the alleged compromise of their confidential information. Accordingly, the court reasoned, the disclosure of the plaintiffs' nonpublic personal information, including user names, passwords, and credit card numbers, constituted ample injury to confer standing to sue. Departing from the majority view, the court found that "the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*." To that court, *Clapper* is consistent with prior Ninth Circuit precedent, finding that Article III's standing requirement was met in the context of a data breach class action. In the wake of the above rulings, federal district courts within the Ninth Circuit—within California in particular—have emerged as the likely venue of choice for a new wave of data breach class actions. In the *Sony Gaming* lawsuit, following the partial denial of Sony's motion to dismiss, the parties reached a preliminarily approved class settlement. The proposed settlement provides unnamed class members with games, subscriptions, and online account credits valued at up to $14 million, and it allows individuals who suffered damages as a result of identity theft to submit a claim for those damages up to a cap of $2,500, subject to an overall cap of $1 million.(The proposed settlement also provides for attorney fees to class counsel of up to $2.75 million.) The final approval hearing is set for May 1, 2015. The *Sony Gaming* settlement's provision of tangible benefits to unnamed class members may be key to obtaining final approval, in light of recent criticism of

privacy class action settlements that provide only *cy pres* relief. For example, in denying review of the Ninth Circuit's approval of a *cy pres* settlement in the non–data breach privacy class action *Lane v. Facebook, Inc.*, Chief Justice Roberts noted that the unnamed class members received "no damages" from the "unusual" settlement fund allocation and acknowledged that the Supreme Court "may need to clarify the limits" on the growing use of *cy pres* remedies in the class action settlement context. *Marek v. Lane*, 134 S. Ct. 8, 9 (2013). In addition to district courts within the Ninth Circuit, federal district courts within the Eleventh Circuit may be among those to watch in connection with data breach class actions. Those courts have yet to address whether *Clapper* effectively overrules the circuit's prior precedent in *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012), which found Article III's standing requirement was met in the context of a data breach class action. The Southern District of Florida's recent final approval of the class action settlement in the *AvMed* litigation may also be of interest, as it provides for cash payments to unnamed class members without any proof that the class member suffered damages as a result of the breach. With data breach claims surviving motions to dismiss in at least some federal district courts, and with companies defending those cases having reached class settlements in lieu of costly and uncertain litigation outcomes, data breach class actions are likely to continue and should remain on corporate counsel's list of litigation risks for 2015. **Republished with permission by the American Bar Association**

Related Practices

Technology
Intellectual Property
Cybersecurity and Privacy

Related Industries

Technology

may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.