The Abundance of Data Breach Class Actions Demonstrates the Importance of Implementing Cybersecurity Protocols and Procedures

by Proud Usahacharoenporn

Class actions stemming from company data breaches continue to proliferate in state and federal courts across the nation. Companies that suffer data breaches potentially face cybersecurity actions from consumers, employees, and even shareholders. Most of these actions are based on allegations that the companies failed to have adequate safeguards and procedures in place to prevent data breaches and to respond to the data breach that has occurred. These cases underscore that companies across all industries should be proactive in implementing sufficient plans and protocols to deal with potential data security breaches, keeping the interests of their employees, customers, and shareholders in mind. Companies that operate across state lines should also be cognizant that different policies may be required in different states, which have varying laws regarding what is required in the event of a data breach.

Local companies recently named in cybersecurity class actions include Lamps Plus, Sprouts Farmers Market, Experian Data Corp., Sony Pictures Entertainment, Inc., and Anthem Blue Cross Life and Health Insurance Co.[i] More of these cases are surviving the law and motion stage, forcing companies to settle cases to avoid protracted litigation. For example, in St. Joseph Health System Medical Information Cases, Orange County Superior Court Case No. JCCP 4716, St. Joseph ultimately settled a class action alleging injuries related to a data breach, which could cost St. Joseph up to $28 million.[ii]

The majority of data breach class actions that do not result in early settlement have been defended on the grounds that the plaintiffs lack the requisite injury required for their claims. Famously, in Spokeo, Inc. v. Robins, 136 S. Ct. 1540, the United States Supreme Court held last year that a consumer alleging the violation of cybersecurity laws must demonstrate an actual concrete injury in order to have standing to sue in federal court and could not rely solely on a bare procedural violation of cybersecurity laws. Lower courts are not in agreement as to how to apply this rule. For example, in Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010), the Ninth Circuit held that injury was adequately alleged where the plaintiffs claimed that they faced an increased risk of future identity theft after a data breach. On the other hand,

other courts have found similar allegations insufficient to establish the requisite Article III injury.[iii]

Due to the uncertainty among the federal courts as to how to apply Spokeo and what it takes to demonstrate injury with respect to cybersecurity class actions in federal court, many plaintiffs' firms will likely end up filing these cases in state court, where the standing and injury requirements are not quite as rigorous, particularly here in California where state laws are among the friendliest to consumers.

---

[i] See, e.g., Varela v. Lamps Plus, Inc., et al., No. 5:16-cv-00577-DMG-KS (C.D. Cal. Mar. 9, 2016) (employee class action); In re: Sprouts Farmers Mkt., Inc., Employee Data Sec. Breach Litig., No. MDL 2731, 2016 WL 5846038 (U.S. Jud. Pan. Mult. Lit. Oct. 6, 2016) (employee class actions); Patton v. Experian Data Corp., No. SACV151871JVSPLAX, 2016 WL 2626801 (C.D. Cal. May 6, 2016) (consumer class action); Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *4 (C.D. Cal. June 15, 2015) (employee class action); Smilow v. Anthem Blue Cross Life & Health Ins. Co., No. CV 15-4556-MWF(AGRX), 2015 WL 4778824, at *1 (C.D. Cal. Aug. 13, 2015) (consumer class action).

[ii] https://topclassactions.com/lawsuit-settlements/lawsuit-news/332917-st-joseph-health-system-medical-data-breach-class-action-settlement/.

[iii] See, e.g., Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012) (holding that increased risk of unauthorized access and identity theft was insufficient to constitute "actual or impending injury"); Reilly v. Ceridian Corp., 664 F.3d 38, 40 (3d Cir. 2011) (holding that increased risk of identity theft was too hypothetical and speculative to establish "certainly impending" injury-in-fact).

Proud Usahacharoenporn
(714) 338-1885
pusaha@rutan.com

To see related articles, please click here.