Articles + Publications | July 26, 2023

EDVA Judge Dismisses Data Breach Class Action for Lack of Article III Standing

Virginia Rocket Docket Blog

RELATED PROFESSIONALS

Dabney J. Carr | Robert A. Angle | Laura Anne Kuykendall

The modern “Information Age” has been defined by rapidly increasing interconnectivity and dependence on the internet by consumers and businesses alike. One side effect of these technological advances has been the increasing frequency of cyberattacks and data breaches perpetrated by sophisticated cyber criminals using ever-evolving methods of infiltration. And, as can be expected, along with the increase in data breaches over the past few decades, we have seen the rise of data breach litigation, and in particular, consumer class action litigation against the companies who have been victimized by those data breaches. The Fourth Circuit has seen several high-profile data breach class actions. Such class actions often face difficult uphill battles in proving the necessary elements for class certification, particularly when it comes to defining a theory of harm that can be proven by common evidence across the class. Last month, Judge Gibney of the Richmond Division of the Eastern District of Virginia dismissed one such data breach class action case for a more basic problem: the named plaintiffs could not demonstrate they had suffered any concrete injury sufficient to establish Article III standing at all, let alone damages that could be proven classwide. *Holmes v. Elephant Ins. Co.*, No. 3:22cv487, 2023 WL 4183380 (E.D. Va. June 26, 2023).

Holmes arose from a data breach affecting Elephant Insurance Company (Elephant), an automobile insurance provider. Cyber criminals exploited Elephant’s auto-populate feature enabled for certain form input fields on the company’s website, allowing them to access the personal information of the plaintiffs and putative class members. The breached information included names, driver’s license numbers, and dates of birth.

Four named plaintiffs brought claims against Elephant on behalf of a putative class under the federal Driver Privacy Protection Act, various state consumer protection and deceptive practices acts, and common law negligence. The plaintiffs alleged that they and the class members had suffered multiple forms of injury, including: (1) an increased risk of harm from future fraud or identity theft, (2) exposure of their driver’s license information for sale on the dark web, (3) a loss of privacy, (4) emotional distress, (5) diminution in the value of their information, and (6) time spent on preventative and mitigative efforts, such as monitoring their credit and financial documents.

Relying on Fourth Circuit precedent, Judge Gibney held that, even accepting the allegations of injury as true, the plaintiffs failed to establish Article III standing. Five out of six of the alleged injuries did not amount to concrete injuries-in-fact at all. Citing the Fourth Circuit’s decision in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017),and the Supreme Court’s decision in *Clapper v. Amnesty Int’l USA*, 568 U.S. 398 (2013), Judge Gibney held that a “heightened risk of future identity theft, without more, does not constitute an injury-in-fact” where the plaintiffs

failed to plead facts supporting their allegations of “certainly impending” future identity theft. Judge Gibney noted the long “chain of possibilities” required to find a threatened injury, which was longer than the “chain of possibilities” the Fourth Circuit rejected in *Beck*: “the Court must assume that the thief targeted Elephant for the PI it contained, then selected the named plaintiffs’ PI from millions of other records, has begun combining the purloined PI with PI obtained from other sources to create a full profile (or ‘fullz’), and will imminently and successfully attempt to use that information to steal the plaintiffs’ identities.” *Holmes*,2023 WL 4183380, at *4.

Judge Gibney also rejected the alleged emotional distress, diminution in value of personal information, and time spent on mitigation as concrete injuries. Regarding diminution in value, Judge Gibney followed the decision of another EDVA judge in a recent data breach class action to hold that barebones assertions of diminution in value of information merely as a result of exposure in a data breach were not sufficient to establish standing. *Id.* at *5 (citing *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 403 (E.D. Va. 2020)). Finally, Judge Gibney held that the plaintiffs lacked standing to pursue declaratory or injunctive relief because their allegations regarding a continued risk of a future breach were conclusory and unsupported. As data breaches continue to occur, litigation will surely follow. This decision from the EDVA will provide valuable guidance to litigators in this unique and evolving area of law.

RELATED INDUSTRIES + PRACTICES

- Business Litigation
- Intellectual Property