Plaintiffs' Attorneys Racing to Courthouses in the United States to File Data Breach Class Actions

Published 22 July 2022

For years, attorneys in the United States have filed class actions after data breaches. However, the frequency of these filings, and the speed in which these cases are filed, are increasing. As one United States federal court observed several years ago, there "*are only two types of companies left in the United States, according to data security experts: 'those that have been hacked and those that don't know they've been hacked.'*"[1] *Another federal court recognized that "data breaches became inescapable features of a digitized world.*"[2]

While in years past companies that experienced a data breach and had to send notice to regulators and impacted individuals might hope they never get sued, now they should fully expect to have a lawsuit filed. The lag time between when the companies sent notice of the breach and a resulting lawsuit has truncated. Now, plaintiffs' attorneys are competing against each other to find a plaintiff (typically an individual who received notice) and race to the courthouse to file a class action lawsuit.

Companies large and small are sued with regularity. Plaintiffs' attorneys know that cyber-insurance is now a standard part of a company's insurance coverage, and this coverage will generally encompass the class action the attorneys file.

Although plaintiffs' attorneys prefer the "ideal" plaintiff who can allege that he or she suffered identity theft or financial fraud, frequent class action complaints do not contain any allegations. The race to the courthouse requires only a plaintiff who received notice. Creative attorneys will allege that the plaintiff suffered a diminished value of his or her personal information, lost time responding to the data breach, experienced anxiety, and are at a risk of future harm because their personal information, protected health information, or both, are in the hands of cybercriminals.

Some courts, particularly federal courts in the United States, have begun to take a harder look at whether plaintiffs who allege no actual identity theft or financial fraud have standing to bring their lawsuit. In 2021, the United States Supreme Court issued a decision in *TransUnion, LLC v. Ramirez*, which narrowed the scope of standing by holding that plaintiffs cannot establish injury in fact to have standing in court by relying entirely on risk of future harm.[3]The United States Supreme Court stated that "*the mere risk of future harm, without more, cannot qualify as a concrete harm in a suit for damages.*"[4]

After the Supreme Court's *TransUnion* decision, and while decisions are divided, numerous federal courts have relied on this decision to dismiss data breach class actions for lack of standing where the plaintiff does not allege actual misuse of their personal information, identity theft or financial fraud.[5] The mere fact that the plaintiff's personal information was implicated in a data breach was not enough to keep the court's doors open. Some federal courts also recognized that the type of data breach could impact the analysis of whether a plaintiff had standing to sue. A court, dismissing a complaint where purely speculative allegations of future injury were pleaded after a ransomware attack, observed that "*the primary purpose of a ransomware attack is the exchange of money for access to personal data, not identity theft.*"[6]

Following the *TransUnion* case and resulting federal cases dismissing data breach class action complaints, plaintiffs' attorneys have flocked to file data breach class action lawsuits in state courts, seeking a reprieve from alleging actual injury as a federal court might require. State courts might have more relaxed pleading standards, courts that are less familiar, or entirely unfamiliar, with data breach class actions, and judges who are more restrained to dismiss data breach class action cases. While procedures exist to remove class actions filed in state courts to federal courts, exceptions apply depending on where the proposed class resides. For example, if at least 2/3 of proposed class members and the defendant reside in the same state, the case cannot be removed.[7] Many businesses, such as those in the medical industry, have an overwhelming majority of their patients in the same state, and may not be able to have a lawsuit removed to federal court.

While there appears to be no looming slowdown in the filing of data breach class actions in the United States, all hope is not lost. These cases are often defensible, and class settlements within a company's existing insurance coverage are frequently achievable when it makes more sense to resolve the case than engaging in a drawn out litigation. Companies can get through the victimization of a data reach and a resulting data breach class action, whether the case is filed in federal or state court. Just don't go through either alone. Increasingly experienced insurance company representatives and defence counsel can help the company at every step.

David M. Ross

Partner, Wilson Elser Moskowitz Edelman & Dicker LLP, Washington, DC Co-Chair, Class Action Practice Team and Cyber Class Action Practice Team

[1] *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015) (citation omitted).

[2] *Blahouse v. Sarrell Reg'l Dental Ctr. For Pub. Health, Inc.*, 2020 U.S. Dist. LEXIS 1225394, *2 (M.D. Ala. July 16, 2020).

[3] *TransUnion, LLC v.* Ramirez, 141 S. Ct. 2190 (2021).

[4] *TransUnion, LLC v.* Ramirez, 141 S. Ct. 2190, 2198-99 (2021).

[5] Examples include: *Quintero v. Metro Santurce, Inc.*, 2021 U.S. Dist. LEXIS 237071 (D.P.R. Dec. 9, 2021); *Aponte v. Northeast Radiology, P.C.*, 2022 U.S. Dist. LEXIS 87982 (S.D.N.Y. May 16, 2022); *In re Practicefirst Data Breach Litigation*, 2022 U.S. Dist. LEXIS 19272 (W.D.N.Y. Feb. 1, 2022); *Cooper v. Bonobos, Inc.*, 2022 U.S. Dist. LEXIS 9469 (S.D.N.Y. Jan. 19, 2022); *Ciccone v. Cavalry Portfolio Services, LLC*, 2021 U.S. Dist. LEXIS 228037 (E.D.N.Y. Nov. 29, 2021); *Baysal v. Midvale Indemnity Co.*, 2022 U.S. Dist. LEXIS 71414 (W.D. Wis. Apr. 19, 2022); *Riordan v. Western Digit. Corp.*, 2022 U.S. Dist. LEXIS 101685 (N.D. Cal. June 7, 2022); *Aviva Kirsten v. California Pizza Kitchen, Inc.*, 2022 U.S. Dist. LEXIS 100652 (C.D. Cal. Mar. 31, 2022); *I.C. v. Zynga, Inc.*, 2021 U.S. Dist. LEXIS 142907 (N.D. Cal. July 30, 2021); *Legg v. Leaders Life Insurance Co.*, U.S. Dist. LEXIS 232833 (W.D. Okla. Dec. 6, 2021).

[6] *In re Practicefirst Data Breach Litig.*, 2022 U.S. Dist. LEXIS 19272, *24 (W.D.N.Y. Feb. 1, 2022).

[7] These removal rules, which fall under the "Class Action Fairness Act," are set forth in 28 U.S.C. § 1332.