Articles + Publications | September 30, 2021

Sued for a Data Breach Out of State? Don't Forget a Personal Jurisdiction Defense

WRITTEN BY

David N. Anthony | Ronald I. Raether Jr. | Timothy J. St. George

This article originally appeared in Pratt's Privacy & Cybersecurity Law Report – October 2021, Vol. 7, No. 8 (LexisNexis A.S. Pratt). It is republished here with permission.

Entities sued for a data breach – even one that is consolidated into a multidistrict litigation proceeding in the defendant's home state – should not forget the personal jurisdiction defense, which can provide a powerful tool to streamline certain legal aspects of the case and ensure that litigation occurs in a defendant's home forum, and not everywhere else.

No business is immune from threats created by cyber criminals and other hackers. In 2020 alone, over 155.8 million individuals were affected by a data breach.[1] Data breaches also continue to cause significant business interruption and cost, many of which now include ransomware as an element of the attack. According to 2020 data, there were 676 breaches that included ransomware as an element of the attack, which was a 100 percent increase as compared to 2019.[2] Further, ransomware attacks made up 81 percent of financially motivated cyberattacks in 2020 and the average cost per breach was $4.44 million.[3]

Lawsuits have always been a possible consequence of a breach, with the frequency of suits increasing as more attorneys join the plaintiffs' bar and courts allow cases to survive motions to dismiss. Frequently, breached entities have consumers who reside across the country. And, plaintiff consumers who have had their data compromised usually wish to sue the breached entity in their home state. Thus, after an entity announces a data breach, it is possible for dozens of lawsuits to be filed in various state and federal courts across the country. Such an occurrence can create significant legal and administrative complications, as it can become extremely burdensome to defend lawsuits all over the country. For example, such a scenario can create a situation where various and divergent choice of law principles can come into play, often pointing to the laws of numerous states, as opposed to being subject to a uniform choice of law analysis.

One potential solution is to move to dismiss out of state cases for lack of personal jurisdiction under the Federal Rule of Civil Procedure 12(b)(2). For plaintiff consumers to bring suit where they respectively reside, there must be personal jurisdiction over the out of state breached entity.

Even if plaintiffs, pursuant to 28 U.S.C. § 1407, move to centralize the litigation into a multidistrict litigation proceeding, the personal jurisdiction defense is still relevant. In a multidistrict litigation proceeding, the transferee court has personal jurisdiction over the defendant only to the same extent as the transferor court.

Thus, the relevant personal jurisdiction inquiry is made by reference to the court where the action was originally filed, even after the case is transferred somewhere else.[4]

Federal Personal Jurisdiction Standards

A federal court may assert either specific or general personal jurisdiction over a breached entity defendant. Unrelated to the allegations of the suit, general personal jurisdiction is based on more persistent contacts with the forum state.[5] This high standard requires a defendant to have continuous and systematic contacts with the forum state, and a plaintiff consumer must be able to show that the forum state is one "in which the corporation is fairly regarded as at home."[6]

For that reason, a breached entity is generally only subject to general personal jurisdiction in its state of incorporation and where its principal place of business is located. To be subject to specific personal jurisdiction, the cause of action must arise out of or relate to the breached entity's contacts with the forum state.[7] A plaintiff consumer must show that the breached entity purposefully established minimum contacts in the forum state, such that it should reasonably anticipate being sued there.[8]

Personal Jurisdiction and Data Breach Litigation

The breached entity's jurisdictional relationship to the forum state must arise out of contacts that the defendant itself created, not that the plaintiff consumer created.[9] A consumer's place of purported injury alone is insufficient.[10] The relevant inquiry focuses on where the alleged acts or omissions by the breached entity occurred, focusing on factors like where the breached entity's technology department is located and where its security team resides.

For example, in *GreenState Credit Union v. Hy-Vee, Inc.*,[11] the plaintiff credit union alleged that the defendant failed to implement adequate data security measures. The plaintiff sued in Minnesota. The defendant breached entity was incorporated in Iowa and had its principal place of business in Iowa.

The court dismissed the action for lack of specific personal jurisdiction. The court noted that the defendant's information technology department, which was responsible for maintaining data security, and its chief technology officer, who was responsible for making decisions regarding data and information security policies and practices, operated out of a facility near defendant's headquarters located in Iowa, not in the forum state of Minnesota.

Likewise, in *Braun v. Mediant Communications, Inc.*,[12] the court also found a lack of personal jurisdiction. In this case, several of the defendant's email accounts were hacked and an email server was compromised, resulting in unauthorized parties gaining access to plaintiff's personal information. Here, the claims arose from an email hack. The defendant presented evidence that its business email is supported, staffed, and maintained in North Carolina.

The court then determined that there was no evidence that any of the defendants actions in Florida gave rise to the claims.

Conclusion

Based on these standards and authority, entities sued for a data breach – even one that is consolidated into a multidistrict litigation proceeding in the defendant's home state – should not forget the personal jurisdiction defense. The relevant inquiry is focused on the breached entity's actions. Thus, the location of the alleged acts or omissions asserted against a breached entity is key when determining personal jurisdiction and can serve as a solution to help a breached entity minimize its litigation risk.

---

[1] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-bynumber-of-breaches-and-records-exposed.

[2] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-data-breaches-point-to-cybersecurity-trends-for-2021.html.

[3] https://atlasvpn.com/blog/ransomware-accounts-for-81-of-all-financially-motivated-cyberattacks-in-2020.

[4] See *In re Showa Denko K.K. L-Tryptophan Prod. Liab. Litig.-II*, 953 F.2d 162, 165 (4th Cir. 1992); accord *In re: Cmty. Health Sys., Inc.*, No. 15-CV-222 (N.D. Ala. Sept. 12, 2016) ("Some of the claims in this case were originally filed in this court and in other federal courts in Alabama, but many of the claims were transferred to this court from other fora to be consolidated into this MDL. The undersigned, as the transferee judge in an MDL, possesses all the jurisdiction and powers over pretrial proceedings in the actions transferred to [her] that the transferor judge would have had in the absence of transfer.").

[5] *ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707, 712 (4th Cir. 2002).

[6] *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 924 (2011); *CFA Inst. v. Inst. of Chartered Fin. Analysts of India*, 551 F.3d 285, 292 n.15 (4th Cir. 2009).

[7] *Fidrych v. Marriott Int'l, Inc.*, 952 F.3d 124, 132 (4th Cir. 2020).

[8] *Perdue Foods LLC v. BRF S.A.*, 814 F.3d 185, 189 (4th Cir. 2016).

[9] *Walden v. Fiore*, 571 U.S. 277, 284 (2014).

[10] *Id*.

[11] No. CV 20-621 (D. Minn. Nov. 10, 2020).

[12] No. 19-62563-CIV (S.D. Fla. Apr. 14, 2020).

RELATED INDUSTRIES + PRACTICES

- Data + Privacy

- Privacy + Cyber