



District of New Jersey Rejects Alter Ego Theory of Liability in Data Breach Class Action

May 01, 2025

Categories:

[Class Action](#)

Authors:

[Caroline E. Oks](#)

In *[In re U.S. Vision Data Breach Litigation](#)*, the District of New Jersey recently dismissed a putative class action related to a 2021 ransomware attack because the plaintiffs failed to adequately allege a direct relationship with the defendant, which was fatal to their claims.

The plaintiffs were patients of Nationwide Optometry, a wholly owned subsidiary of defendants U.S. Vision, Inc. and USV Optical, Inc. (collectively, "USV") until USV sold Nationwide in 2019. The plaintiffs alleged that after the sale, USV retained personally identifiable information (PII) and protected health information (PHI) of Nationwide's patients and that Nationwide functioned as USV's alter ego. Between April 20, 2021, and May 17, 2021, USV experienced a data breach compromising PII and PHI of more than 711,000 individuals. The plaintiffs claimed the data breach caused them to suffer identity theft risks, financial damages, and loss of privacy. The lawsuit asserted claims for negligence, breach of fiduciary duty, breach of contract, unjust enrichment, and violations of consumer protection laws.

The defendants moved to dismiss, arguing that (1) merely storing the plaintiffs' data does not create the direct relationship with them required for their fiduciary-duty, implied-contract, unjust-enrichment, consumer-fraud, and negligence claims; and (2) the plaintiffs failed to allege sufficient facts to plausibly suggest that USV and Nationwide are alter egos.

The district court agreed that the plaintiffs failed to establish a direct relationship with USV and therefore dismissed the complaint, holding that some level of connection was required for the plaintiffs' claims. Because no such connection was adequately alleged, USV could be liable only if it was an alter ego of Nationwide, which did have a direct relationship with the plaintiffs. At the time of the breach, USV was continuing to store the plaintiffs' data, but, as the

court found, “Plaintiffs were patients of Nationwide and there is no indication that they were even aware of USV’s relationship with Nationwide, let alone reviewed and relied on USV’s privacy policy and practices before providing their information to Nationwide” or “even knew that USV would be storing Plaintiffs’ information or that it was a consideration of Plaintiffs before they provided their PII/PHI to Nationwide.”

The court also held that the plaintiffs’ bare-boned allegations of common control failed to state a plausible alter-ego claim. Prior to the sale in 2019 and nearly two years before the data breach, the plaintiffs pled just one shared common officer and a shared computer system between USV and Nationwide. After the sale in 2019, and at the relevant time of the data breach in 2021, the plaintiffs simply alleged that USV continued to store their PII/PHI. These facts fell woefully short of suggesting that USV dominated Nationwide, the court held; moreover, alleging partial common ownership and potentially intertwined business operations was insufficient to state an alter-ego claim under Third Circuit precedent.

Additionally, the court dismissed without prejudice the plaintiffs’ breach-of-contract claim because the alleged contract between USV and Nationwide to provide data-storage and data-security services for Nationwide was not attached to the complaint or the motion. Accordingly, the court dismissed as conclusory the plaintiffs’ allegation that they were the intended third-party beneficiaries of the contract with any right to enforce it.

This decision reins in the often far-reaching potential for liability for data-breach claims.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.