GROOM LAW GROUP

www.groom.com

Cybertheft Lawsuit: Court Dismisses Fiduciary Breach Claims Against Plan Sponsor for a Second Time

PUBLISHED: March 11, 2021

On February 8, 2021, in the latest turn in the saga of a closely-watched ERISA cybersecurity lawsuit, the Northern District of Illinois again dismissed fiduciary breach claims against Abbott Laboratories ("Abbott Labs") relating to the cyber theft of $245,000 from a participant's account in the Abbott Laboratories Stock Retirement Plan (the "Plan"). The decision marks the second time the court has dismissed claims against Abbott Labs.

Previously, on October 2, 2020, the court granted Abbott Labs' motion to dismiss upon its finding that the plaintiff failed to demonstrate that Abbott Labs was a fiduciary to the Plan, as well as its finding that the plaintiff failed to demonstrate that the Abbott Labs officer who served as the plan administrator (who the court agreed was a fiduciary) breached his fiduciary duties. Notably, the court permitted both ERISA claims and state law claims to proceed against the Plan's recordkeeper, Alight Solutions, LLC ("Alight"), which is currently the sole defendant in the lawsuit. Following its unsuccessful effort to dismiss the claims filed against it, on November 6, 2020, Alight filed an answer to the complaint. In that filing, Alight generally agreed with the plaintiff's description of the manner and method of the theft but denied that it was a fiduciary to the Plan and otherwise denied any liability for the plaintiff's losses.[1]

Following the dismissal of Abbott Labs, the plaintiff filed an amended complaint in which she added allegations to revive the ERISA claims against

If you have any questions, please do not hesitate to contact your regular Groom attorney or the authors listed below:

Allison Itami
aitami@groom.com
(202) 861-0159

Michael Kreps
mkreps@groom.com
(202) 861-5415

David Levine
dlevine@groom.com
(202) 861-5436

Arsalan Malik
amalik@groom.com
(202) 861-6658

Anthony Onuoha
aonuoha@groom.com
(202) 861-2609

[1] Among other defenses, Alight argues that at all times, it "reasonably acted in good faith, and did not undertake any conduct that was malicious, egregious, in bad faith, grossly negligent, or in willful or reckless disregard," and that "any damages were caused by people and/or events other than Alight."

Abbott Labs. As discussed below, the court found that the ERISA claims against Abbott Labs were still insufficient even in light of the new allegations.

For a full recap of the court's prior decision and the facts of the case, please see our prior client alerts here and here.

I. Court's Analysis

The court's analysis centered on whether the plaintiff had sufficiently alleged that Abbott Labs breached its duty of prudence and duty to monitor Alight based on several new allegations in the amended complaint. In this regard, the plaintiff alleged that Abbott Labs breached its duties when initially hiring Alight and subsequently renewing its contract despite several cybersecurity and data privacy incidents involving Alight and its predecessor company, which she argued Abbott Labs knew or should have known.

Specifically, the plaintiff identified the following incidents:

- In 2013, Aon Hewitt (Alight's predecessor company) and other financial institutions were targeted by an international cybercrime ring, resulting in the theft of millions of dollars.
- In 2015, a manual mailing error at Aon Hewitt resulted in the disclosure of client information to an unintended recipient. Also, in 2015, presumably due to some type of technical glitch, participants in a benefits program were able to access personal information about other participants.
- In 2016, an unknown person accessed sensitive personal records of 2,892 individuals (including social security numbers). Also, in 2016, in reference to the Estée Lauder cybersecurity litigation [Groom Alert: New Case Raises Difficult Questions About ERISA Remedies for 401(k) Account Thefts], Alight allegedly "allowed an unauthorized user to initiate three separate transfers from a 401(k) retirement account belonging to someone else. The transfers totaled $99,000."
- In 2019, Alight disclosed that emails and URLs for certain Alight websites inadvertently included personal information, including Social Security Numbers. Also, in 2019, it became publicly known that the U.S. Department of Labor was investigating Alight's cybersecurity practices.

A. Duty of Prudence

Citing the foregoing incidents, the plaintiff claimed that Abbott Labs breached its duty of prudence both when hiring Alight in 2003 and when renewing its contract in 2015. The court rejected both claims.

First, with respect to Alight's initial hiring, the court noted that "the incidents referenced in her amended complaint occurred after Alight was first offered the job." Thus, the court concluded that it "cannot infer that the Abbott Defendants breached their duty of prudence by hiring Alight in 2003 based on events a decade later."

Second, with respect to Alight's contract renewal, the court noted that although two of the identified incidents occurred prior to the renewal, the events were "limited in size and scope," "did not involve significant lapses in security protocols," and that "no client funds were stolen" as part of the incidents. The court also emphasized that none of the referenced incidents involved Alight's performance on behalf of the Plan (i.e., they related to Alight itself or other clients).

Notably, the court further noted that "[a]lthough an investigation by the Abbott Defendants in 2015 would have shown that two isolated incidents occurred under Aon Hewitt's watch, Aon Hewitt presumably handled tens of thousands of customer transactions that year, and rehiring a plan administrator with a less-than-perfect track record does not plausibly allege imprudent conduct."

B. Duty to Monitor

The plaintiff also sought to revitalize her claims that Abbott Labs breached its duty to monitor Alight based on the referenced incidents. In rejecting the monitoring claims, the court emphasized that, despite the fact that Abbott Labs may have had knowledge of Alight's previous incidents with cybersecurity, the duty to monitor is plan-specific. The court further noted that "[t]he duty to monitor requires fiduciaries to keep track of how an administrator performs for their own plan, not others." Under this view, the court concluded that it "cannot reasonably infer that the Abbott Defendants breached their duty to monitor based on incidents that did not involve them" and that "[w]hether the Abbott Defendants knew about these incidents does not change this conclusion."

Additionally, the court noted that although the plaintiff suggested that Abbott Labs may have known about Alight's "lax attitude toward data security," the plaintiff had "not alleged any action by the Abbott Defendants plausibly showing that they failed to monitor Alight's performance as it relates to the Abbott Labs Stock Retirement Plan specifically."

II. Conclusion

While Abbott Labs has again defeated the plaintiff's claims, it is not yet out of the woods as the dismissal is without prejudice. The court has also required Abbott Labs to complete its document production as part of the discovery process notwithstanding the dismissal. Further, the court has extended the deadline for the plaintiff to file an amended complaint to 30 days following the completion of Abbott Labs' document production, which is expected to occur in the summer. Thus, this may not be the final chapter.

As far as takeaways, while the latest dismissal is a helpful decision from a plan sponsor perspective, it serves as yet another reminder of the continuing importance of cybersecurity in the ERISA space. As cybersecurity threats against retirement accounts continue to increase, plan sponsors should ensure they have an understanding of service provider cybersecurity practices, and that they continue to monitor such practices.