GROOM LAW GROUP

Publications

Cybertheft Lawsuit: ERISA Fiduciary Breach Claims Dismissed Against Plan Sponsor but Move Forward Against Recordkeeper

ATTORNEYS & PROFESSIONALS

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

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

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

PUBLISHED
10/16/2020

SERVICES

Employers & Sponsors
- Retirement Programs
- Fiduciary & Plan Governance Litigation
- Employer & Sponsor Litigation

Retirement Services
- Retirement Services Litigation
- Plan Services & Providers

On October 2, 2020, the Northern District of Illinois ruled on motions to dismiss in a closely-watched cybertheft lawsuit arising out of the theft of $245,000 from a participant's account in the Abbott Laboratories Stock Retirement Plan (the "Plan").[1] The plaintiff alleged that the plan sponsor Abbott Laboratories ("Abbott Labs"), an Abbott Labs officer who served as the Plan's named fiduciary and administrator ("Administrator"), and the Plan's recordkeeper Alight Solutions, LLC ("Alight") breached their fiduciary duties under ERISA in failing to prevent the cybertheft.

For the court, the determinative issue at this stage of the litigation was the fiduciary status of each of the defendants. As described below, the court concluded that Alight was the only defendant sufficiently alleged to be a fiduciary, and thus dismissed all claims against the Abbott Labs defendants but allowed the claims against Alight to move forward. The case highlights the evolving nature of ERISA cyber-security litigation and represents the second case where plaintiffs survived a motion to dismiss alleging that plan service providers were fiduciaries when allegedly failing to prevent cyberfraud from draining participant accounts (see *Leventhal v. MandMarblestone Group LLC*).

I. Background

The complaint was filed in April 2020 and recounts the successful efforts of an unknown individual (the "Cyber Thief") to compromise the plaintiff's Plan account. The complaint describes numerous interactions between the Cyber Thief and Alight—which, in addition to operating the Plan's participant website and phone line, was responsible for managing distributions—that the plaintiff alleges facilitated the theft.

The mechanics of the cybertheft are described in detail in the complaint but consisted of the following steps, according to the plaintiff:

- First, the Cyber Thief clicked the "forgot password" option on the Plan's website, which generated an authentication code that was sent to the plaintiff's email address.

- Second, having already compromised the plaintiff's email account, the Cyber Thief retrieved the authentication code and used it to successfully access the plaintiff's Plan account.
- Third, upon gaining access to the Plan account, the Cyber Thief changed the account password and also added a new, previously unassociated SunTrust Bank account as a distribution option for the account funds.
- Lastly, after seven days had passed in accordance with Alight's wait period for transfers to new accounts, Alight complied with the Cyber Thief request to distribute $245,000 from the plaintiff's Plan account to the new SunTrust Bank account.[2]

II. Claims Dismissed Against Abbott Labs

The court rejected the plaintiff's allegations that Abbott Labs acted as a "functional fiduciary" to the Plan. In this regard, the court noted that the plaintiff's allegations were conclusory and that "[t]he complaint fails to allege any fiduciary acts taken by Abbott Labs, no less link them to the alleged theft." Thus, the court dismissed the fiduciary breach claims against Abbott Labs.

The court also considered the fiduciary status of the Administrator. In contrast to Abbott Labs, the court noted that the Administrator was clearly a fiduciary given the Administrator's role under the terms of the Plan. Since there was "no dispute" about the threshold fiduciary question, the court proceeded to consider each of the plaintiff's claims against the Administrator.

First, the plaintiff claimed that the Administrator breached the Administrator's duty of loyalty because the Plan's website "misrepresents how plan assets are administered and safeguarded." In dismissing this claim, the court noted that because Alight was responsible for maintaining the Plan's website, the court "cannot infer that [the Administrator] misled plan participants through a website he does not operate."

Second, the plaintiff claimed that the Administrator breached the Administrator's duty of prudence by failing to protect the plaintiff from the cybertheft. In this regard, the plaintiff alleged that the duty of prudence applies to the "safeguarding of data and prevention of scams." In dismissing this claim, the court noted that the plaintiff failed to support this characterization of the duty of prudence with any authorities. In addition, the court noted that while there was Second Circuit precedent that supported a finding of imprudence when a fiduciary fails to address a *known* risk, in this case, the plaintiff had not "allege[d] that [the Administrator] knew about the unauthorized attempts to access" the plaintiff's account.

Lastly, the plaintiff claimed that the Administrator breached the Administrator's duty to monitor other fiduciaries (i.e., Alight), including their "distribution processes, protocols, and activities." In dismissing this claim, the court noted that the plaintiff "does not allege any monitoring process between [the Administrator] and Alight, let alone a defect in that process." Further, the court noted that the plaintiff's allegations concerning Alight's own protocols do not "speak to [the Administrator] or his duty to monitor Alight."

III. Claims Move Forward Against Alight

Alight argued that the plaintiff's claims that it was a fiduciary were conclusory and that, in any event, it was not a fiduciary to the Plan because it performed "ministerial functions" that were not fiduciary in nature. Notably, Alight's defense focused solely on the threshold question of its fiduciary status, and Alight did not (for purposes of its motion to dismiss) contest the breach and causation elements of the plaintiff's ERISA claim.

In refusing to dismiss the claims against Alight, the court stated that the plaintiff's claims were "far more" than conclusory. Specifically, the court noted that "[t]he complaint catalogues the repeated actions taken by Alight related to the Retirement Plan and its assets, including, most importantly, the disbursement of $245,000 in plan assets." The court further noted that such actions were sufficient to "infer that Alight acted as a fiduciary by exercising discretionary control or authority over the plan's assets."

Apart from permitting the plaintiff's ERISA claims to move forward, the court also sustained a portion of the plaintiff's claims against Alight regarding violations of the Illinois Consumer Fraud and Deceptive Practices Act ("ICFA"). As a threshold matter, the court first concluded that the ICFA claims were not preempted by ERISA because they sought "recovery for activities that occurred outside the terms of the plan." Then, although the court concluded that the plaintiff had failed to allege a claim of a "deceptive act" under the ICFA, the court found that the plaintiff had sufficiently alleged a claim for an unfair business practice relating to Alight's failure "to protect Bartnett's personal information and properly notify her of important changes to her account."

IV. Implications

As described in our previous client alert, the *Bartnett* case serves as another reminder of the importance of maintaining sound cybersecurity and data protection practices. There are important lessons to be drawn for everyone in the retirement space, including plan sponsors, service providers, and participants themselves.

That said, this latest development in the case has particular importance for recordkeepers similar to Alight. Although recordkeeper functions have generally been viewed as non-fiduciary, "ministerial" functions, the court credited plaintiff's allegation that Alight exercised discretionary control or authority over plan assets as a result of its role in maintaining the Plan's call center and website, and its responsibility for administering distributions.

While the court's siding with the plaintiff is not necessarily surprising at the motion to dismiss stage—where it is required to resolve inferences in favor of the plaintiff—it will be important to monitor this case to see how the court's analysis develops on the question of recordkeeper fiduciary status. We note that it would be a significant departure from existing authorities if the court were to conclude that certain standard recordkeeper functions constitute fiduciary conduct.