THE WAGNER LAW GROUP

LAW ALERT
July 7, 2020

Plan Sponsor and Service Provider Submit Dueling Motions to Dismiss in Response to Data Breach Suit

Further demonstrating the lack of clarity on who is liable when a plan suffers a data breach, on June 30th, Abbott Laboratories and Alight Solutions, pointed fingers at each other in dueling motions to dismiss a complaint that alleged both were fiduciaries in connection with a plan data breach that stole $245,000 from a participant's plan account. The Northern District of Illinois will now have to decide if, based on the complaint's allegations, either Abbott or Alight (or both) could have (i) fiduciary responsibility with respect to the theft of funds from the participant's account and whether (ii) the plan participant has pled a plausible claim of fiduciary breach.

The Original Complaint and DOL Investigation of Alight Solutions

The motions to dismiss stem from a complaint filed on April 3, 2020, by Heide Bartnett, a participant in the Abbott Corporate Benefits Stock Retirement Plan. In the complaint, Ms. Bartnett sued her employer, Abbott Laboratories, the purported plan administrator, "Abbott Corporate Benefits," the Plan itself, and Abbott employee, Marlon Sullivan. Ms. Bartnett also sued Alight Solutions, the Plan's "contract administrator" and record keeper.

Specifically, the complaint alleged that Defendants breached their fiduciary duties in (i) failing to verify the identity of Ms. Barnett prior to making distributions to a cybercriminal; (ii) failing to establish distribution processes to safeguard the Plan's assets from unauthorized withdrawals; and (iii) failing to monitor other fiduciaries' distribution "processes, protocols, and activities." Ms. Barnett also sued Alight for violation of the Illinois Consumer Fraud and Deceptive Practices Act.

The timing of the complaint was fortuitous for Ms. Barnett. Only three days after she filed the complaint, the DOL revealed it was investigating Alight for the processing of unauthorized distributions as a result of cybersecurity breaches. In support of the DOL's petition to compel Alight's production of documents in response to its subpoena, the DOL stated that:

> EBSA discovered that Alight processed unauthorized distributions as a result of cybersecurity breaches relating to its ERISA plan clients' accounts. Further, in violation of its service provider agreements, Alight failed to immediately report cybersecurity breaches and the related unauthorized distributions to ERISA plan clients after its discoveries. In some instances, Alight failed to disclose cybersecurity breaches and unauthorized distributions to its ERISA plan clients for months, if at all. Alight also repeatedly failed to restore the unauthorized distribution amounts to its ERISA plan clients' accounts.

Scalia v. Alight Solutions, Case: 1:20-cv-02138, Dkt No. 1.1 (N.D. Ill. April 6, 2020).

These are heavy allegations that tie to the facts and circumstances of the *Bartnett* case. The DOL, however, has not yet intervened in Ms. Bartnett's case nor given any indication it will do so.

The Dueling Motions To Dismiss Disclaim Fiduciary Status In Connection With The Data Breach

In response to Ms. Bartnett's complaint, both Alight and the Abbott affiliated Defendants, filed motions to dismiss that disclaimed any liability for fiduciary breach. First, Alight attempted to persuade the Court its responsibilities were only ministerial in nature and according to the terms of its service provider contract with the Plan: "the Administrative Services Agreement between Abbott and Alight…states that in providing benefit plan administration services, Alight is not a fiduciary under ERISA with respect to the Plan. That agreement also states that Alight does not have any discretionary control with respect to the investment of Plan assets or administration of the Plan."

Notably, the complaint alleged Alight provided contract administration, record-keeping, and information management services for the Plan but Alight's motion to dismiss stated it merely provided ministerial record keeping services to the Plan. The true scope of Alight's responsibilities might be fleshed out in the Administrative Services Agreement which Alight has filed under seal with the Court.

To head off any argument it acted as a functional fiduciary, Alight claimed it possessed no power or discretion in distributing funds to participants. Rather, Alight suggested it is the *participants* of the Plan who have the power to direct their distributions: "By Plaintiff's own pleading concession, it is the Plan participants who direct the distribution of benefits from their accounts." This argument, however, doesn't exactly square with ERISA §404 which expressly requires plan fiduciaries who control the administration and distribution of plan assets (not the beneficiaries of the plan) to exercise their powers in a prudent and loyal fashion.

Abbott, in turn, pointed its finger back at Alight. It argued that the complaint's allegations only targeted Alight as having the power to direct distributions and perform identify verifications and, therefore, Abbott could not be held liable as a fiduciary and committed no breach because "the only factual allegations are against Alight." Additionally, according to the Abbott affiliated Defendants, the complaint did not allege that "any part of the process for selecting and retaining Alight was deficient." And, Abbott also targeted the complaint's failure to plead causation noting that there could be no causal connection between any of its actions and the theft of funds.

The Motions To Dismiss Point Out Ambiguities In The Complaint

While it is premature (until Ms. Bartnett responds to the motions to dismiss) to predict how the Court might hold, one thing is true: the original complaint did not clearly delineate who the named and functional fiduciaries of the Plan are with references to the governing Plan documents. The complaint, for example, listed the following Defendants as fiduciaries:

- Abbott Laboratories (Plan Sponsor and functional fiduciary of Plan)
- "Abbott Corporate Benefits" (Plan Sponsor and Named fiduciary of the Plan)
- Marlon Sullivan (Named Plan Administrator and the Named Sponsor) of the Plan
- Alight Solutions ("contract administrator," record keeper and functional fiduciary).

The complaint, in listing out Defendants and why they are fiduciaries did not cite to the governing Plan documents, Form 5500's, or the Administrative Services Agreement. Without these frames of reference, it might be difficult for the Court to decipher which entity/person was responsible for what. Abbott's motion to dismiss touched on these ambiguities in stating that the complaint was conclusory and did not plead facts to show it acted as/or possessed the power of a fiduciary in connection with distributions to participants. Abbott's motion to dismiss also explained that "Abbott Corporate Benefits" does not exist as a legal entity and suggested Ms. Bartnett's inclusion of them as a Defendant appears to be based on a misreading of the Plan's Form 5500.

It will be interesting to see how Ms. Bartnett and her counsel respond to these arguments in either oppositions to motion to dismiss or an amended complaint.

Why Carefully Written Plan Documents and Service Provider Agreements are Essential for Plan Sponsors

Clearly, Abbott and Alight can't both be right. At the very least, one of them is responsible for the administration of plan assets to participants under ERISA. Under ERISA § 402(a)(1), a retirement plan written document must include one or more "named fiduciaries" who control and manage the plan's operation and administration of the plan—including distributing the plan's assets to participants. And this provision exists because, in drafting ERISA, Congress intended responsibility for managing and operating a plan—and liability for mismanagement—to be focused with a degree of certainty.

To avoid needless and potentially harmful imprecision, plan documents should be drafted with ERISA best practices in mind with an eye towards specifying, to a degree of certainty, fiduciary responsibility. In the context of cybersecurity, best practices for plan sponsors could include:

- Reviewing plan service provider agreements to identify cybersecurity fiduciary liability and any indemnification or limits of liability provisions.
- Reviewing the cybersecurity processes and procedures utilized by plan service providers concerning data exchange and cybersecurity processes and procedures.
- Confirming plan service providers have appropriate professional liability and cyber liability insurance coverage.

Reviewing the plan service provider's Service Organization Control Reports. A Service Control Report provides an internal controls report on the services provided to the plan to assess and address the potential risks associated with an outsourced service.

Of most critical importance is ensuring a plan is governed by carefully worded plan documents with clear delineation of responsibilities and liability subject to indemnification. As we have recently seen in the pending case *Leventhal v. MandMarblestone Group, LLC* (E.D. Pa), fiduciary status and liability are not so easily discerned with respect to cyber security breaches. In *Leventhal*, the Court held that both the plan sponsor, and the plan's TPA/record keeper, could have acted as ERISA fiduciaries because (i) the plan sponsor was alleged to be "careless" in its "computer/IT systems" and "employment policies" in permitting an employee and plan participant to work remotely without adequate safeguards to do so, and (ii) the TPA/ recordkeeper could have failed to act with the requisite prudence and diligence when they observed

the "peculiar nature" and "high frequency" of the withdrawal requests and failed to implement "typical" procedures and safeguards to notify participants and/or verify the requests. [See our Law Alert covering the *Leventhal* case here].

In an already novel confrontation under ERISA fiduciary law—where there are few if any bright line rules as to who is a fiduciary with respect to data breaches—the outcome of cases like Abbott and Leventhal will most likely be highly fact-specific, case by case, and dependent upon the powers possessed and delegated pursuant to the governing plan documents.

Before an incident arises, plan sponsors and plan service providers should proactively address issues of cybersecurity in more detail with their ERISA counsel.

www.wagnerlawgroup.com

@wagner-law-group
fb.com/WagnerLawGroup

Boston:
99 Summer Street, 13th Floor
Boston, MA 02110
Tel: (617) 357-5200

@wagnerlawgroup
@wagnerlawgroup

Boynton Beach:
1880 N. Congress Avenue, Suite 200
Boynton Beach, FL 33426
Tel: (561) 293-3590

Chicago:
180 N. LaSalle Street, Suite 3200
Chicago, IL 60601
Tel: (847) 990-9034

Lincoln, MA:
55 Old Bedford Road, Suite 303
Lincoln, MA 01773
Tel: (617) 532-8080

New York:
200 Park Avenue, Suite 1700
New York, NY 10166
Tel: (212) 338-5159

San Diego:
8677 Villa La Jolla Drive, Suite 888
San Diego, CA 92037
Tel: (619) 232-8702

San Francisco:
315 Montgomery Street, Suite 900
San Francisco, CA 94104
Tel: (415) 625-0002

St. Louis:
1099 Milwaukee Street, Suite 140
St. Louis, MO 63122
Tel: (314) 236-0065

Tampa:
101 East Kennedy Boulevard, Suite 2140
Tampa, FL 33602
Tel: (813) 603-2959

Washington, D.C.:
800 Connecticut Avenue, N.W., Suite 810
Washington, D.C. 20006
Tel: (202) 969-2800