Abbott Data Breach Suit Provides Lessons For Plan Sponsors to Protect Against Potential Liability

*Jordan Mamorsky**

On April 3, 2020, a participant in the Abbott Corporate Benefits Stock Retirement Plan, Heide Bartnett, filed a complaint against her employer, Abbott Laboratories, the Plan administrator, the Plan itself, an Abbott employee and Alight Solutions, the Plan's contract administrator and recordkeeper, for allegedly processing a fraudulent $245,000 distribution from Ms. Bartnett's Plan account to an unknown person that impersonated her. In response and further demonstrating the lack of clarity on who is liable when a plan suffers a data breach, on June 30, 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 the Plan data breach. The U.S. District Court for 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: (1) fiduciary responsibility with respect to the theft of funds from the participant's account, and whether (2) the plan participant pled a plausible claim of fiduciary breach.

THE FACTS OF THE ORIGINAL COMPLAINT

The following chronology of facts contained in Ms. Bartnett's complaint provide a good example of how, practically, things can go wrong when a cyber thief gains access to plan participant personal information:

According to Ms. Bartnett's complaint:

- On or about December 29, 2018, a cyber thief accessed Ms. Bartnett's individual Plan account via the Plan's Internet Website and chose the "forgot password" option.
- Because the cyber thief already had obtained Ms. Bartnett's personal information, it inputted the last four digits of Ms. Bartnett's Social Security number and her date of birth to create a new password to gain access to Ms. Bartnett's account.
- After accessing Ms. Bartnett's account with a new password, the cyber thief changed Ms. Bartnett's bank account direct deposit information to a different SunTrust bank account.

*JORDAN D. MAMORSKY is an experienced litigator and has served as counsel in well-publicized cases involving ERISA fiduciary duty and prohibited transaction matters. He regularly represents plan sponsors, plan fiduciaries, financial advisors, plan participants, company executives, third-party administrators, employers, and others in a broad range of ERISA disputes, including breach of fiduciary duty, denial of benefit, Employee Stock Ownership Plan, and deferred compensation matters. He received his Juris Doctor from New York Law School, a Bachelor of Science from Vanderbilt University, and completed a Postdoctoral Fellowship in Corporate Governance and Business Ethics at Yale University. He is admitted to practice law in New York, New Jersey, and Massachusetts. Mr. Mamorsky can be contacted at jmamorsky@wagnerlawgroup.com.

- Two days later, on December 31, 2018, the cyber thief contacted the Abbott Benefits Service Center, impersonating Ms. Bartnett from a phone number that she had never called from before, to request a withdrawal of money from the account.

- The customer service representative explained that the newly added SunTrust bank account must be on file for seven days before money could be withdrawn from Ms. Bartnett's account.

- Eight days later, on January 8, 2019, the cyber thief called the Abbott Benefits Support Center seeking to withdraw the funds. To verify the identity of the supposed "Ms. Bartnett," the Support Center sent another one-time code to Ms. Bartnett's email address, which the cyber thief verified.

- Upon this identify verification procedure, the cyber thief withdrew $245,000 to the new bank account it had added to Ms. Bartnett's Plan account.

Based on the substance of these allegations, Ms. Bartnett's complaint alleged that all defendants (the Abbott affiliated defendants and Alight) breached their fiduciary duties. The complaint specifically averred that in: (1) failing to verify the identity of Ms. Barnett prior to making distributions to a cybercriminal; (2) failing to establish distribution processes to safeguard the Plan's assets from unauthorized withdrawals; and (3) failing to monitor other fiduciaries' distribution "processes, protocols, and activities," the defendants' breached their fiduciary responsibilities under Section 404 of the Employee Retirement Income Security Act of 1974 (ERISA). 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 Department of Labor (DOL) revealed it was investigating Alight for the processing of unauthorized distributions as a result of cybersecurity breaches. The DOL noted that its investigation had uncovered that Alight failed to immediately report cybersecurity breaches and the related unauthorized distributions to ERISA plan clients after its discoveries. And, that in some instances, Alight failed to disclose cybersecurity breaches and unauthorized distributions to its ERISA plan clients for months, if at all. In support of the DOL's petition to compel Alight's production of documents in response to its subpoena, the DOL stated that:[1]

> 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.

While the preliminary findings of this investigation clearly weigh on the allegations in Ms. Bartnett's case, the DOL has not yet intervened in Ms. Bartnett's case nor given any indication it will do so.

THE COMPETING 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 competing motions to dismiss that disclaimed any liability for fiduciary breach. First, Alight attempted to persuade the court its responsibilities were only ministerial in nature 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, recordkeeping, and information management services for the Plan, but Alight's motion to dismiss stated it merely provided ministerial recordkeeping 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 odd argument, however, does not 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 prudent discretion in administration of plan assets.

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." Also, according to Abbott and the Abbott affiliated defendants, the complaint did not allege that "any part of the process for selecting and retaining Alight was deficient." 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," recordkeeper and functional fiduciary).

The complaint, in listing out defendants and why they are fiduciaries, did not cite to any governing Plan documents, Form 5500's, or the Administrative Services Agreement. Without these frames of reference, it is difficult 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/or possessed the power as 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.

Identification of fiduciary responsibilities in the service provider agreement will be critical because an express delegation of fiduciary duties can help support a finding of who might serve and function as a fiduciary of an ERISA plan. For example, in *Leventhal v. Mand-Marblestone Grp. LLC*,[2] the court found that because the service provider agreement with the plan's recordkeeper, Nationwide, delegated to "general administrative responsibilities" that include the ability to "[t]ake all other acts necessary for the proper administration of the Account," Nationwide could have ERISA fiduciary responsibilities with respect to exercising authority or control in disposing of, and managing the Plan's assets.

THE IMPORTANCE OF PLAN SPONSOR'S MONITORING PLAN SERVICE PROVIDERS

Based on the DOL's public disclosure of its investigation of Alight, it will be interesting how the ERISA fiduciary duty to monitor comes into play with respect to any actions the Abbott affiliated defendants could have taken to monitor Alight's conduct. The DOL investigation of the Abbott plan's service provider should provide a warning sign for plan sponsors to carefully monitor the actions of their service providers, particularity in the cyber security context.

To be clear, pursuant to ERISA §§ 404 and 405(c)(2), plan sponsors can incur liability when they fail to carefully select or monitor the service provider, and that service provider then breaches a delegated ERISA fiduciary duty.[3]

The DOL also believes this to be an important issue, and even dedicates a stand-alone Web page to provide "tips" to plan sponsors on selecting and monitoring service providers.[4]

Part of the DOL recommendations that are relevant in the cybersecurity context are to:

- Periodically review the performance of your service providers to ensure that they are providing the services in a manner and at a cost consistent with the agreements.
- Review plan participant comments or any complaints about the services, and periodically ask whether there have been any changes in the information you received from the service provider prior to hiring (for example, does the provider continue to maintain any required state or federal licenses).
- If the service provider will handle plan assets, check to make sure that the provider has a fidelity bond (a type of insurance that protects the plan against loss resulting from fraudulent or dishonest acts).

WHY CAREFULLY WRITTEN PLAN DOCUMENTS AND SERVICE PROVIDER AGREEMENTS ARE ESSENTIAL FOR PLAN SPONSORS

Clearly, Abbott and Alight cannot 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 the plan—and liability for mismanagement—to be focused with a degree of certainty.

To avoid needless and po-

tentially 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 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 its service providers data exchange and cybersecurity processes and procedures.
- Confirming the service providers have appropriate professional liability and cyber liability insurance coverages.
- Reviewing the service provider's Service Organization Control Reports.

Of most critical importance is ensuring a plan is governed by carefully worded plan documents with delineation of responsibilities and liability subject to indemnification. As we have recently seen in the pending case *Leventhal v. Mand-Marblestone Group, LLC*., fiduciary status and liability can be far-reaching. In *Leventhal*, the court held that both the plan sponsor and the plan's third-party administrator/ recordkeeper could have acted as ERISA fiduciaries because: (1) 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 (2) the third-party administrator/ 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.

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 factually specific, case by case, and sourced from the powers possessed and delegated pursuant to the governing plan documents and in function pursuant to ERISA § 3(21).

PLAN SPONSORS WHO UTILIZE THE NEW DOL ELECTRONIC DISCLOSURE SAFE HARBOR SHOULD ENSURE THEY ARE COMFORTABLE WITH CYBER SECURITY PROTECTIONS

On May 21, 2020, the DOL issued a new rule titled "Default Electronic Disclosure by Employee Pension Benefit Plans under ERISA." The rule provides safe harbor relief to plan administrators who satisfy specific conditions in delivering electronic communications. The DOL emphasized the cost savings associated with the rule in that it "expects the rule to enhance the effectiveness of ERISA disclosures and significantly reduce the costs and burden associated with furnishing many of the recurring and most costly disclosures."

The administration cost savings associated with the new rule are obvious and beneficial to the industry. But keep in mind that this rule allows a plan administrator to send ERISA mandated disclosures directly to a covered individual's email address, rather than posting the documents to a Website. According to the rule, the email itself must only contain certain content that the notice of Internet availability would otherwise provide and meet certain requirements that

would otherwise apply to the Website and the documents described in the rule.

Therefore, before plan sponsors make use of this cost-saving and efficient mode of communication, it should have comfort—particularly in light of the fraud that occurred in *Abbott*—that its email communications with participants are secure. This is also important because the DOL wrote in its new regulations that it "expects that many plan administrators, or their service or investment providers, already have secure systems in place to protect covered individuals' personal information. Such systems should reduce covered individuals' exposure to data breaches."

To help meet the DOL's expectation and enhance the cybersecurity of their employee benefit plans, employers should contact ERISA counsel to guide them through a thorough review and the implementation of necessary cybersecurity measures.

NOTES:

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

[2]Leventhal v. MandMarblestone Group LLC, 2019 Employee Benefits Cas. (BNA) 158856, 2019 WL 1953247 (E.D. Pa. 2019).

[3]See, for example, Moitoso v. FMR LLC, 2020 WL 1495938, at *10 (D. Mass. 2020), citing 29 U.S.C.A. §§ 1104, 1105(c)(2).

[4]See https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/fact-sheets/tips-for-selecting-and-monitoring-service-providers.pdf.