

## COVID-19, Publications

# New Lawsuit Alleges Fiduciary Breaches by Plan Sponsor and Recordkeeper for Quarter Million Dollar Cybertheft

## ATTORNEYS &amp; PROFESSIONALS

**Jim Cole**[jcole@groom.com](mailto:jcole@groom.com)

202-861-0175

**David Levine**[dlevine@groom.com](mailto:dlevine@groom.com)

202-861-5436

**Arsalan Malik**[amalik@groom.com](mailto:amalik@groom.com)

202-861-6658

**George Sepsakos**[gsepsakos@groom.com](mailto:gsepsakos@groom.com)

202-861-0182

**Kevin L. Walsh**[kw Walsh@groom.com](mailto:kw Walsh@groom.com)

202-861-6645

## PUBLISHED

04/16/2020

## SOURCE

COVID-19 Resource

## SERVICES

- [Retirement Programs](#)
- [Fiduciary & Plan Governance](#)
- [Plan Services & Providers](#)

## Brief Takeaway

As a result of the Coronavirus Aid, Relief, and Economic Security Act (“CARES Act”), plan sponsors and service providers across the country are bracing for a flurry of participant activity with respect to distributions, loans, and other account transactions. Many plan sponsors and service providers are actively working to support participants by facilitating access to retirement account funds through COVID-19 related loans and hardship distributions. However, it is important to recognize that the uptick in participant distribution and loan activity also presents an opportunity for cybercriminals and fraudsters to take advantage.

A recently-filed lawsuit, [\*Bartnett v. Abbott Laboratories et al.\*, No. 2020 CV 2127, \(N.D. Ill. filed April 3, 2020\)](#), describes in specific detail the efforts cybercriminals often take to pilfer assets from retirement accounts. As a complaint, the filing provides only the plaintiff’s version of what happened, and we have not yet heard from the defendants. But the complaint is particularly interesting in its description of how the theft occurred, and may point to some useful approaches to try to reduce future fraud. The complaint also illustrates that cybersecurity over retirement accounts is not limited to the systems and records of the plan sponsor and the recordkeeper; cybersecurity at the individual participant level is also critical.

## I. Introduction

On April 3, 2020, a participant in the Abbott Laboratories Stock Retirement Plan (the “Plan”) filed a lawsuit against Abbott Laboratories and Abbott Corporate Benefits, the individual designated as the plan administrator, and the Plan’s recordkeeper, Alight Solutions, LLC (“Alight”) alleging the defendants failed to use the level of care, skill, prudence, and diligence required of an ERISA fiduciary to protect the plaintiff’s plan assets. These alleged breaches allowed an individual (the “Cyber Thief”) to steal \$245,000 from the plaintiff’s account, according to her complaint.

The complaint describes detailed factual allegations regarding the efforts of the Cyber Thief to compromise the plaintiff's account, as well as the interactions between the Cyber Thief and Alight, which operated the Plan's participant website and phone line and was responsible for issuing plan distributions. The complaint notes that the basis of these allegations is an internal investigation report prepared by Alight that was turned over to local law enforcement in response to a subpoena, and then subsequently obtained by the plaintiff.

## II. Overview of the Alleged Cyber Theft

### *Cyber Thief's Interactions with Defendants*

According to the complaint, the Cyber Thief already had certain personal information about the plaintiff before attempting to access the participant's Plan account, including the last four digits of her social security number and her date of birth. The Cyber Thief presumably also had access to her email to receive the authentication codes.

On December 29, 2018, the Cyber Thief attempted to login to the plaintiff's Plan account by clicking the "forgot password" option on the participant website. The Cyber Thief entered the last-four digits of her social security number and birthdate. This triggered a security prompt which allegedly offered the Cyber Thief the option to either answer certain security questions or receive a one-time verification code by email. The Cyber Thief elected the latter option, and successfully passed the security screening.

Upon gaining access to the plaintiff's account, the Cyber Thief changed the account password and added direct deposit information for an unknown SunTrust bank account to the plaintiff's account.

Two days later, an unknown person (presumably, the Cyber Thief or an accomplice) called the participant phone line from a phone number not previously associated with the participant's account and reported being unsuccessful in processing a distribution online. The interaction did not result in a distribution being issued, as Alight required a seven-day waiting period between adding a new account and allowing distributions to that new account.

Eight days later, on January 8, the Cyber Thief called the participant phone line again and requested a distribution from the plaintiff's account. The plaintiff alleges that rather than requiring the caller to address security questions, the Alight representative sent another one-time code to the plaintiff's email address. After the Cyber Thief's validation of the one-time code, the plaintiff alleges that the defendants "authorized \$245,000 to be transferred from Ms. Barnett's account to the SunTrust Bank account." It is unclear what happened to the \$245,000 after it was transferred to the SunTrust account, but presumably large amounts of funds were subsequently transferred to other accounts controlled by the Cyber Thief, as SunTrust Bank was only able to recover \$59,494.02, according to the complaint. The 20% tax withholding on the \$245,000 distribution was also recovered.

### *Plaintiff's Interactions with Defendants*

Throughout the complaint, the plaintiff claims that despite her alleged preference to receive notices about account activity by email, the defendants sent notices relevant to the theft by regular mail.

The plaintiff alleges that the defendants notified her about the addition of the SunTrust Bank account by regular mail. The plaintiff alleges that the delay caused by sending the notice by regular mail precluded her "opportunity to question the addition of the SunTrust Bank account before any unauthorized withdrawals were made from her Plan account."

Similarly, the plaintiff alleges that following the initiation of the unauthorized transfer of \$245,000 on January 8<sup>th</sup>, the defendants again sent notice by regular mail. The plaintiff alleges that had the defendants sent notice by email, the plaintiff "would have been able to halt the transfer and would have stopped the transfer."

Notably, the complaint also states that days after the Cyber Thief gained access to the plaintiff's online account and changed her password, the plaintiff's husband—after successfully answering security questions—regained access to the online account and changed the password. The complaint notes that the plaintiff was notified via email of these changes, which suggests that her email account may have been compromised, with the Cyber Thief possibly intercepting prior communications when the Cyber Thief was aware his or her actions triggered email notices.

The plaintiff notes that she discovered and reported the theft to the plan sponsor on January 15 (one day after the funds were transferred to the SunTrust Bank account), and that the defendants subsequently froze the account and advised the plaintiff to contact law enforcement.

### *Investigation*

Local law enforcement in Illinois initiated an investigation into the theft, which involved issuing subpoenas to the plan sponsor, Alight, and SunTrust Bank for materials relating to the transfer of funds. The complaint notes that “SunTrust was unable to locate records for the account holder.” In addition, law enforcement traced the IP address that had been used to access the plaintiff’s account, which revealed that the Cyber Thief may have been located in India.

## III. Implications

### *Greater Cybersecurity Risks in the Pandemic Era*

The *Bartnett* case provides another reminder that retirement accounts are not immune to cyberattacks. [See Groom Alert: [New Case Raises Difficult Questions About ERISA Remedies for 401\(k\) Account Thefts](#)]. In fact, retirement accounts may be particularly attractive targets for cybercriminals given the significant amount of assets held in such accounts.

In this new pandemic era, cybersecurity threats are greater than ever as millions of people across the world employ technology at unprecedented levels for business and personal matters. But while millions are practicing social distancing, cybercriminals continue to employ a variety of fraudulent means, which includes deceptive methods like those used in the *Bartnett* case—to defraud and steal.

Notably, in response to the growing threats, on April 15, 2020, the Department of Labor’s Office of Inspector General included imposter schemes to obtain benefit plan distributions in its list of investigative focus areas.

### *Considerations for Fiduciaries and Service Providers*

The *Bartnett* case provides reminders of several important considerations that might be incorporated into plan processes:

First, plan fiduciaries responsible for plan administration are well served to understand how account activity is triggered (*e.g.*, additions of permitted bank accounts, phone numbers). Plan fiduciaries could also evaluate whether there are other practical practices that could balance the need for accessibility to funds with the protection of plan participants.

Second, plan fiduciaries and service providers can collaborate to implement processes to safeguard information. Plan fiduciaries can also review service providers’ cyber security capabilities and procedures at the RFP stage as well as during their ongoing monitoring process. It is important to remember that there may be no one “right” way to implement safeguards and each plan, with its own unique participant demographics, may have its own interests to balance.

Third, although plan fiduciaries and service providers are not obligated to educate participants about cybersecurity, and are not required to create documents like a data security or privacy statement, it may benefit a plan and its participants to provide education on cybersecurity to help ensure that participants are part of the process of protecting access to a participant’s account. The complaint suggests that it was the hacking of the plaintiff’s own personal computer and email account that may have led to the retirement account being accessed.

Fourth, plan fiduciaries and service providers can review their insurance policies (*e.g.*, fiduciary insurance, cyber insurance) and fidelity bonds for scope of coverage and other guarantees. In particular, a close review of such policies can be beneficial to understand the scope of coverage, including whether social engineering or fraud losses like those described in *Bartnett* are covered.

While the complaint in *Bartnett* is styled as a breach of fiduciary duty claim under ERISA that would presumably fall within the coverage of a fiduciary insurance policy (barring any exclusions), claims for loss from cyber fraud will not necessarily always be brought as ERISA fiduciary claims. In those situations, plans often look to their cyber insurance policy or fidelity bond for coverage of losses where a proper individual authorizes a transfer of funds but is criminally induced to do so by an impersonator on the telephone or by email. However, some cyber insurance policies and fidelity bonds do not cover social engineering losses unless special endorsements are added. To avoid unpleasant surprises later on, plan sponsors and plan fiduciaries can work with their counsel and insurance brokers to make sure that the desired coverage is included in their respective insurance policies and fidelity bond.

[New-Lawsuit-Alleges-Fiduciary-Breaches-by-Plan-Sponsor-and-Recordkeeper-for-Quarter-Million-Dollar-Cybertheft](#)