

# Cyber Suits Highlight 401(k) Record-Keeper Best Practices

By Carol Buckmann (August 2, 2022)

The army of internet thieves doesn't spare retirement plans. For example, several lawsuits have been filed against plan sponsors and their record-keepers, including Estee Lauder Inc., Abbott Laboratories,[1] and the companies' record-keeper Alight Solutions Inc., as a result of theft of plan accounts.

Those cases have not resulted in final decisions clearly defining the cybersecurity responsibilities of fiduciaries and service providers, but a newly filed lawsuit against Colgate-Palmolive Co. and Alight provides another opportunity to do so.[2]



Carol Buckmann

While the U.S. Department of Labor has not issued regulations defining responsibilities for protecting plan assets from thieves and hackers, it has released a package of best-practice recommendations for plan sponsors and record-keepers. These recommendations include third-party audits of cybersecurity procedures and multifactor authentication.

However, the cases filed make the point that call center employees are a vulnerable part of any record-keeper system, and that they must be properly trained to consult managers or secure additional identifying information before putting through any suspicious transactions.

## **Disberry v. Colgate-Palmolive**

In *Disberry v. Employee Relations Committee of the Colgate-Palmolive Co.*, a participant whose entire account worth over \$750,000 was stolen by a hacker has sued the plan committee, Alight and custodian Bank of New York Mellon — all of whom are alleged to be fiduciaries — in the U.S. District Court for the Southern District of New York, to get the account restored with attorney fees and costs.

The complaint focuses on the specific actions of Alight and its employees. Although the alleged breach did not involve BNY Mellon employees, the complaint also cites provisions of the BNY Mellon agreement requiring BNY Mellon to maintain an information security program and to protect sensitive information against unauthorized access. The participant alleges that the plan committee rejected her benefit claim and will not restore her losses resulting from the fiduciary breach.

## ***401(k) Red Flags***

The facts as recited in the complaint read like an example of why record-keepers need better employee training and strict identification procedures.

After several unsuccessful attempts to process changes online, a thief called the Alight call center to change the password, email, address and bank account information for the participant's account. No notice of the change was sent to the participant's prior email address or telephone number. The mailing address was not in the same country as the other contacts.

A temporary password was mailed to the participant but without notifying the participant by email or text that a temporary password had been requested and mailed out. The mail was

intercepted by the thief.

Although the summary plan description indicated that there would be a 14-day wait before a distribution would be made following an address change, no such waiting period was imposed, and an immediate lump sum distribution was quickly made. The participant did not discover the theft until she checked her account balance, and alleges that she was told that the loss was unfortunate but that the plan benefit "was paid in accordance with Plan terms and requirements."

### ***Defined Benefit Plan Procedures Prevented the Theft***

The plaintiff alleges that the thief also tried unsuccessfully to access her pension under Colgate-Palmolive's defined benefit plan, which was administered by a different record-keeper. That record-keeper insisted on a photo ID, which the thief was unable to provide.

### **Separate Litigation Involving Alight**

On a separate front, the Department of Labor has been battling Alight in court over its investigation of Alight's cybersecurity procedures. The U.S. District Court for the Northern District of Illinois has ruled that Alight must respond to the DOL's subpoena seeking documents relating to the unauthorized distribution of plan assets,[3] though Alight has appealed in the U.S. Court of Appeals for the Seventh Circuit.[4]

Alight is also seeking an order preventing the DOL from sharing the information with other federal agencies, which could result in their own enforcement action.

### **Who Should Be Responsible?**

There is as yet no single federal law setting cybersecurity standards or providing for protections when accounts are stolen by hackers. It is unlikely criminal authorities will be unable to restore this loss, so who should be responsible — the service providers and fiduciaries responsible for hiring and monitoring the record-keeper, or an innocent participant?

The Employee Retirement Income Security Act provides that fiduciaries can be personally liable for losses from breaches of their responsibilities. However, trustees, even if fiduciaries for some purposes, do not generally have a duty to inquire into instructions to make distributions.

Charges that Alight acted as a discretionary fiduciary here may also present a hurdle, as most record-keepers are not fiduciaries.

However, the fiduciary committee would appear to have a responsibility to hire plan service providers with adequate cyber-theft protections. As the case progresses, the committee's knowledge and monitoring of Alight's procedures and its questionable statement that payment had been made to the thief in accordance with proper procedures are likely to be issues.

Whether the plan sponsor maintained insurance or attempted to get indemnification for the loss on behalf of the participant under its service agreements may also be reviewed.

## Steps to Provide Better Protection

Plan sponsors can take steps now to reduce the probability a theft like this will harm participants. Here are some practices recommended by the DOL and experts:


- Require that record-keepers maintain cybersecurity insurance and have their procedures audited regularly by outside parties. Put these obligations in service agreements.
- Maintain cybersecurity insurance and have procedures audited because thefts can also result from hacking into employee computers at the worksite or when working remotely.
- Whenever contact information is changed, send texts and e-mail notices immediately using the prior contact information and alerting the participants to contact the record-keeper immediately if they did not initiate the changes.
- Impose a mandatory delay on payment of any distributions requested immediately after a change in contact information.
- Require confirmation of identity beyond passwords, such as the photo ID requirement imposed by Colgate-Palmolive's defined benefit plan provider or specific personal identifiers.

We need a federal solution to protect participant accounts. Binding DOL guidance on legal liability in this area is sorely needed, but the best solution may be action by Congress to provide for specific participant remedies. Such a provision could even be tacked onto the pension reform legislation currently being considered by Congress.

---

*Carol Buckmann is a founding partner at Cohen & Buckmann PC.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] *Berman v. Estee Lauder Inc.*, 419 cv-06489, N.D. Cal, which has been settled; *Bartnett v. Abbott Laboratories* , 492 F. Supp. 3d 787 (N.D. Ill., 2020) and 2021 WL 428820 (N.D. Ill., 2021).

[2] *Disberry v. Emp. Rel. Comm. of the Colgate-Palmolive Company*, S.D.N.Y. No. 22-cv-05778.

[3] *Martin J. Walsh v. Alight Solutions Inc.*, 1:20-cv-2138, N.D. Ill.

[4] Appeal filed Dec. 10, 2021.