

Colgate-Palmolive 401(k) Theft Case Settles on Undisclosed Terms, Leaving Open Questions

Victoria E. Anderson

September 19, 2024

Many who work with defined contribution plan administrators and consult plan sponsors on their ERISA fiduciary duties have been carefully monitoring *Disberry v. Employee Relations Committee of the Colgate-Palmolive Company et. al.* The case came to a conclusion recently with an undisclosed settlement and, importantly, without the court conclusively opining on fiduciary process or whether any party is responsible for restoring assets stolen from a participant's 401(k) plan account.

The case alleged that plan sponsor Colgate-Palmolive Company ("Colgate") and its plan recordkeeper, Alight Solutions ("Alight"), breached their fiduciary duties when more than \$750,000 was stolen from a former Colgate employee's 401(k) account. (The court granted a motion to dismiss by a third defendant, the plan's custodian, Bank of New York Mellon ("BNY Mellon"), on the grounds that the plaintiff did not plead a link between any actions of BNY Mellon and the fraudulent conduct alleged in the complaint, and therefore did not establish that BNY Mellon acted as a fiduciary.) The plaintiff in the suit claimed in her complaint that a fraudster pretending to be her duped Alight, changed her contact information and bank account information, and requested an immediate cash distribution of her entire plan account. The complaint accuses the defendants of violating ERISA by ignoring numerous significant red flags (such as the fact that the fraudster changed the plaintiff's contact information such that the phone number and email address were from one country and the mailing address was from another), failing to follow their own procedures (such as waiting 14 days after an address change before processing and distributing a participant's account), and failing to implement reasonable procedures to detect and prevent fraud and theft of plan assets.

Since the suit was filed in July 2022, employee benefits attorneys have been awaiting the court's decision, as a verdict in the plaintiff's favor would have meant a substantial increase in risk for retirement plan sponsors (or recordkeepers, or both), who would potentially be on the hook for plan participant losses resulting from incidents like the one in the Colgate suit. Now that the parties have settled, it appears that there will not be a final word on the matter from the court after all.

Especially because there is no definitive ruling on the issue, plan sponsors and recordkeepers should be sure to have processes and controls in place to ensure that they are in compliance with their fiduciary duties with respect to account security. For example, they should consider the following:

- Limit access to participant account information to designated employees.
- Conduct periodic security awareness training for their employees.

- Implement strong access control procedures (such as multi-factor authentication) to ensure that plan participants are who they say they are.
- Continue to follow the [Department of Labor's cybersecurity guidelines issued in 2021](#).

Finally, plan sponsors should exercise prudence in selecting and managing third-party service providers. For example, they should examine whether their service agreements require their service providers to do the following:

- Have robust information security policies and procedures in place to protect confidential information against unauthorized access and use.
- Obtain annual outside audits to confirm compliance with information security policies and procedures.
- Have insurance policies that would cover losses caused by security and identity theft breaches.
- Indemnify the plan sponsor for financial losses resulting from security and identity theft breaches.
- In the event of a security or identity theft breach, immediately notify the plan sponsor and affected plan participants, and cooperate with the plan sponsor to investigate and address the cause of the breach.