LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Cybersecurity Breach Suits Benefits Lawyers Should Watch

By **Kellie Mejdrich**

Law360 (July 22, 2022, 7:48 PM EDT) -- Attempts to steal workers' personal information and even their retirement savings are on the rise, attorneys say, raising questions about plans' and third-party administrators' exposure for cybersecurity breaches under federal benefits law.

Earlier this month, a retiree sued her former employer Colgate-Palmolive under the Employee Retirement Income Security Act, alleging plan fiduciaries breached their duties by failing to prevent a fraudster from hijacking her 401(k) account.

In addition to that suit, benefits lawyers say they are keeping an eye on large class actions pending in New York and Georgia against third-party plan administrators claiming injury over leaked personal information.

The U.S. Government Accountability Office in a February 2021 report warned about increased legal risks to ERISA plan fiduciaries stemming from cyber breaches, pointing to recent lawsuits alleging that cyberattacks resulted in unauthorized distributions from retirement plan accounts.

The GAO warned in its report that outsourcing retirement plan administration to third parties — something increasingly common for many employers — could boost opportunities for malicious individuals to gain unauthorized access.

Bailey & Glasser LLP partner Mark G. Boyko said that ERISA could prove to be a potent tool for plaintiffs in this burgeoning field of litigation.

"I just think this is going to be a growing area. I think it's only a matter of time before there are larger-scale successful hacks that actually succeed in removing large amounts of participant assets from a plan," he said. "In that situation, I think that ERISA is going to be probably the strongest tool that the participants have to protect themselves from that."

Here are four cases that could shed light on companies' responsibilities when it comes to protecting retirement plan participants from online intruders.

Colgate-Palmolive Plan Sued Over Drained 401(k)

Paula Disberry, a retired Colgate-Palmolive marketing executive, sued her former employer and other companies involved with her 401(k) retirement plan on July 7 in New York federal court, seeking to recoup losses after a thief took over her account and drained it of more than $750,000 in value.

The case is significant for benefits attorneys because similar challenges brought by individuals under ERISA seeking to restore plan assets resulting from cyber intrusions have settled. Significant settlements included a closely watched 2020 challenge brought against Abbott Laboratories as well as a 2019 suit against Estee Lauder Inc., each from individual retirees alleging plan fiduciaries breached their ERISA duties by allowing unauthorized distributions from their accounts.

Disberry, a South African resident who first became eligible to participate in the company 401(k) plan in 1998, alleges the company's employee relations committee, benefits administration company Alight Solutions and plan trustee The Bank of New York Mellon were fiduciaries of the plan and breached their duties under ERISA by allowing an unauthorized distribution from her account.

Disberry said in the complaint she learned in September 2020 that her account had been drained of its entire balance in a single taxable lump sum in March of that year. A fraudster in Las Vegas was the culprit, Disberry said, who had contacted Alight in January 2020, falsely impersonated her and requested the company mail a temporary personal identification number to her address in South Africa. The fraudster ultimately intercepted that mail and used the PIN to take over her retirement account credentials, later mailing the plan distribution to a newly added Las Vegas address.

Disberry seeks relief in the form of restored plan losses and investment earnings, as well as attorney fees and costs.

"We feel confident that the ERISA claims will stick," said Kirsten Scott, partner with Renaker Hasselman Scott LLP and attorney for Disberry.

"Each of the defendants that we've named in the case exercised authority or control with respect to the management of or disposition of plan assets, or they had discretionary responsibility in administering the pension plan," Scott said.

Elliot D. Raff, member at McDonald Hopkins LLC, said issues in the Disberry case demonstrate the range of liability faced by employers and other companies involved in benefit plan administration.

"Employers need to be thinking about, what kind of ERISA fiduciary record have they made? Because if I'm Mrs. Disberry, I'm suing everybody," Raff said.

The case is Disberry v. Employee Relations Committee of the Colgate-Palmolive Co. et al., case number 1:22-cv-05778, in the U.S. District Court for the Southern District of New York.

DOL Authority Challenge Pending

The Seventh Circuit could soon rule on a challenge brought by Alight Solutions to the U.S. Department of Labor's authority to investigate cybersecurity breaches, after a three-judge panel heard oral **arguments in April** in the company's appeal of a court-ordered subpoena in a cybersecurity-focused investigation.

The DOL first requested information from Alight in 2019, which provides record-keeping and administrative services for more than 750 employee benefit plans serving around 20.3 million people, as part of an investigation into whether cybersecurity breaches resulted in unauthorized distributions from ERISA plan accounts.

Alight appealed to the Seventh Circuit in December after the DOL obtained a subpoena enforcement order for the information in Illinois federal court, arguing that cybersecurity — and investigating Alight for nonfiduciary acts — fell outside the scope of the DOL's authority under ERISA. Alight asked the circuit panel to overturn the subpoena, which the district court refused to stay pending the appeal.

Earlier this month, a federal magistrate judge in Illinois overseeing the district case **approved a protective order** limiting how federal agencies can share information obtained in the DOL's investigation.

Ivelisse Berio LeBeau, partner with the Wagner Law Group, said she's keeping a close eye on the appeal.

"I think it underscores the DOL's authority to investigate, regarding cybersecurity breaches and benefit plans," Berio LeBeau said.

"I think the guidance last year that was issued was a sign that they're interested. The [Employment Benefits Security Administration] has made no secret that they are concerned. Because, frankly, there's a whole lot of personally identifying information and a whole lot of assets related to employee benefit plans," Berio LeBeau said.

The case is Martin Walsh v. Alight Solutions LLC, case number 21-3290, in the U.S. Court of Appeals

for the Seventh Circuit.

Workers Target 401(k) Record-keepers

Employee 401(k) plan participant Eric Giannini seeks to represent thousands in a proposed class action after benefits administration company Transamerica Retirement Solutions notified him that his personal data was stolen in a 2021 cybersecurity breach.

Giannini first sued in New York federal court in December on behalf of "individual retirement fund plan participants who used Transamerica's services and had their sensitive [personally identifying information] accessed by unauthorized parties because of a lapse in network security in or around June of 2021." He alleged he was a victim of identity theft after hackers stole his personal information including his address, Social Security number, figures related to retirement plan distributions, and tax information.

Giannini's complaint largely asserts state tort claims and doesn't seek relief under ERISA, which is typical of many cases involving personal information obtained through employee benefit plan administrators.

Giannini alleged he already experienced fraudulent purchase requests and spam calls, but alleged he and other class members would experience "a slew of harms" in the future resulting from the breach, including fraudulent charges and targeted advertising without their consent.

Claims alleged against the company include negligence, breach of contract and unjust enrichment. The complaint also alleges the security lapses violated numerous state consumer protection and data security laws including in California and New York.

Giannini seeks more than $5 million in damages as well as an injunction against the company prohibiting it from misusing private information and requiring it to issue prompt, complete and accurate disclosures; changes in the company's cybersecurity policies; and a minimum of three years of credit monitoring services for affected class members.

Raff of McDonald Hopkins said cases like the one brought by Giannini show the high risks facing plan record-keepers.

"They're in a bind, because they are spending hundreds upon hundreds of millions of dollars a year for artificial intelligence systems ... systems after systems after systems to flag and identify potential cyber crooks," Raff said of record-keepers. "And yet the cyber folks are always a step ahead, because there's money to be had."

Raff said he's learned from conversations with big record-keeping firms that hackers often target a company with sets of records that can include thousands of employees.

"They have learned how to program multiple network computers to take those data sets and throw it at the big record-keepers," he said, with many of those accounts often password-protected with phrases or keywords that might be easily guessed.

"So, the cyber thieves have come to understand that it doesn't take a lot of data to steal someone's 401(k) account and have a good chance at a big payday," he added.

The case is Giannini v. Transamerica Retirement Solutions LLC, case number 7:21-cv-10282, in the U.S. District Court for the Southern District of New York.

Workers Sue Over Massive Benefits Administration Breach

Benefit plan consulting firm Horizon Actuarial Services LLC faces a consolidated mega-class of more than 2.5 million people after a Georgia federal judge agreed in **May** to combine five class actions over a November 2021 data breach.

According to a consolidated complaint from April, the data breach resulted in the leak of sensitive information from plan participants in more than two dozen employee benefit plans, including

numerous multi-employer plans.

Like the Transamerica case, the Horizon consolidated class action does not bring ERISA claims but involves employee benefit plan participants seeking legal remedies.

The cases are Sherwood v. Horizon Actuarial Services LLC, case number 1:22-cv-01495; Quan v. Horizon Actuarial Services LLC, case number 1:22-cv-01531; Bedont v. Horizon Actuarial Services LLC, case number 1:22-cv-01565; Torrano v. Horizon Actuarial Services LLC, case number 1:22-cv-01674; and Hill v. Horizon Actuarial Services LLC, case number 1:22-cv-01676, in the U.S. District Court for the Northern District of Georgia.

--Editing by Bruce Goldman.
