COMPLIANCE | November 9, 2020

Cybersecurity Risks Still Lurking for Retirement Plan Sponsors

A recent federal court decision does not let plan sponsors off the hook, and various state laws may be applied to cases against them.

Reported by LEE BARNEY | *Art by* STEVEN COMPTON

PLAN SPONSORS MIGHT THINK THEY can breathe a sigh of relief following a recent decision from U.S. District Judge Thomas Durkin for the Northern District of Illinois. The decision dismissed Abbott Laboratories from a lawsuit related to a cybersecurity theft from an employee's retirement account, ruling that the plan participant failed to prove that Abbott itself is a fiduciary with regard to the alleged failures.

Susan Rees, of counsel at The Wagner Law Group, calls the decision "provisional" and says she expects the participant could be able to correct pleading errors by "focusing on the actual fiduciaries and plan administrator." In other words, the judge took Abbott off the hook for procedural reasons, Rees says. "One of the things this court also got wrong is about the application of the prudence requirement of Section 404(a) of ERISA [the Employee Retirement Income Security Act] to plan cybersecurity protection," Rees says. "Contrary to this court's view, the DOL [Department of Labor], in the preamble to the DOL's recent electronic disclosure safe harbor regulation, clearly articulated that plan administrators or other responsible plan fiduciaries must assume they have a fiduciary duty to have a prudent cybersecurity protocol and to monitor any service provider that has access to participant data or assets."

While it might have been good news for plan sponsors, it was not for their service providers. In the same decision, Durkin held that the lawsuit can be brought under ERISA against the Abbott plan's recordkeeper, Alight Solutions, as a "functional" fiduciary, and that Alight Solutions may also be liable under a state consumer protection law.

This decision could get corrected, and Abbott could get pulled back in, either under the general principle that the Abbott plan administrator is responsible for what its recordkeepers, third-party administrators and other vendors do, or perhaps, as in another recent cybersecurity case, as being jointly responsible with the service provider for the breach.

"The industry will be watching this case, fraught with unanswered questions, both legal and factual," says Rees, who advises plan sponsors and administrators to be vigilant about their cybersecurity protocols for ERISA purposes, but also to be aware that some ERISA cybersecurity cases may involve state law claims. "Although yet another unanswered question for the courts, every plan counsel needs to be cognizant that state laws may be applied."

Enrico Schaefer, a trial attorney with Traverse Legal, says that, given the fact that retirement plan sponsors handle sensitive participant data and accounts, it is just plain common sense that they should be extremely careful about handling that information.

"Courts are increasingly willing to hold companies that hold and manage customer data accountable for breaches

Kristy Brown, a partner, co-chair of the litigation practice and chair of the cybersecurity litigation team at Alston & Bird, says that while there have been only a few, high-profile cybersecurity lawsuits brought against retirement plans, there could be many more due to the growing concerns all companies have about cybersecurity risks. "It is generally fair to say that there is an explosion of data breach class action lawsuits being brought against all industries and types of data," Brown says. "There is no exception to this with respect to retirement plans, whose sensitive data includes participants' names, dates of birth, Social Security numbers and addresses. All companies that handle sensitive data are at risk, which only increases with people working virtually from home during the pandemic."

Most of the cases being brought about cybersecurity breaches deal with negligence, Brown says. Plan sponsors can protect themselves from such theft by undertaking "reasonable security measures to protect their plan's data, including overseeing the protocols at service providers," she says. "Cases will focus on things that run the gamut from how the service provider was selected to vendor management—what auditing and vetting procedures were applied to ensure the plan was reasonably secured."

Thus, Brown says, sponsors' "cyber preparedness should have them thinking on the front end about mitigating such risk and how to respond if an incident is discovered." Companies should be prepared to go through what is called a "tabletop exercise, whereby all of the key stakeholders, with the help of their legal team, run through hypothetical incidents to see if there are any weaknesses in their plan or disconnects."

The next thing plan sponsors should do is to examine their contracts with third parties to make sure they include indemnification provisions that spell out the vendor's responsibilities in the event of a data breach—most important of which is how much the vendor would pay in the event of a breach, including legal costs, Brown says.

Finally, she says, plan sponsors need cybersecurity insurance.

Tags retirement plan cybersecurity

Reported by Lee Barney

Art by Steven Compton

Reprints Please contact the PLANSPONSOR Reprint Manager, Michelle Judkins.

You Might Also Like:

COMPLIANCE | October 5th, 2020

Abbott Defendants Dismissed From Retirement Plan Cybersecurity Lawsuit

COMPLIANCE | July 20th, 2020

Alleged Boeing Retirement Plan Fraudster Charged in California

COMPLIANCE | May 29th, 2020

Court Finds Plan Sponsor Could Be Found Liable for Retirement Plan Cyberfraud