CERITY PARTNERS®

Cybersecurity & Retirement Plans
Minimizing Plan Sponsor Fiduciary Responsibility

June 8, 2020

Key Takeaways

- The size and long-term nature of retirement accounts have made them a prime target for cybertheft.
- The Department of Labor has been silent on whether participant data qualifies as a plan asset in the event of a breach.
- Plan sponsors need to develop a prudent cybersecurity process to protect their participants and mitigate their fiduciary risk.

With millions of Americans now in a virtual work environment, cybertheft is top of mind for most businesses and organizations. But this risk has always been present. Prior to the onset of COVID-19, cybersecurity breaches were already increasing. And for retirement plan sponsors, there is an extra need for caution.

A Cautionary Tale

In April, a breach of fiduciary duty complaint was filed against Abbott Laboratories and its recordkeeper, Alight Solutions, following a $245,000 unauthorized distribution from a participant's account.

The case centers around whether a participant's account is considered a plan asset in the instance of a cybersecurity breach, and whether the plan sponsor failed to uphold its fiduciary duties. While ERISA (Employee Retirement Income Security Act) holds plan sponsors to the highest fiduciary standards, it is silent regarding cybersecurity breaches. Without regulatory guidance, it is difficult for plan sponsors to determine what responsibilities they have in protecting their participants' personal information.

While the outcome is still pending, this case and the lack of regulatory guidance underscore the importance of having a prudent process that helps mitigate your fiduciary liability in the event of a similar incident. So, what should you do?

Six Steps to Help Reduce Your Fiduciary Liability

Regardless of whether participant data is considered a plan asset, it's important to approach this issue prudently, as you would any plan decision. Here are six steps you can take to help protect your participants' personal information and manage the associated risk:

1. Request information from your service providers regarding their cybersecurity protocols. You want to make sure they have the appropriate safeguards in place as well as a documented process for preventing and addressing security breaches.

2. Review your service agreements. Where necessary, ask vendors to add language that includes a specific commitment to cybersecurity insurance, indemnification language regarding losses and damages, and a communication strategy in the event of a cybersecurity breach.

CERITY PARTNERS®

3. Limit the amount of participant data you share with vendors, providing only the necessary information to service your plan and your participants.

4. Acquire cyber insurance to help address the financial implications of a breach, such as the restoration of funds for affected participants.

5. Review your fidelity bond and fiduciary insurance to confirm the coverage amount is sufficient and covers forgery, computer fraud, and funds transfer fraud.

6. Train staff and employees on cybersecurity best practices. They are your first line of defense. The more they understand the risks, the more likely they are to sense when a request or email doesn't pass the "sniff test."

Additionally, you might consider outsourcing cybersecurity to a third-party expert who can help you create, execute and monitor your cybersecurity policy.

Proactive Vigilance

Cybercriminals are becoming bolder in their approach. Plan sponsors need to be just as vigilant with protecting their participants' personal information and retirement savings. While each breach is unique, the steps outlined above provide a solid foundation for mitigating your fiduciary liability. Contact a Cerity Partners advisor to learn more.