Wednesday, June 2, 2021

Cybersecurity: Retirement Plan Sponsors Can Protect Themselves

The digital world has opened many doors—including some to theft and the abuse of information. When it comes to retirement plans and participant assets, cybersecurity has emerged as a significant area of focus. Read on to find out how plan sponsors can protect themselves and their participants while meeting fiduciary obligations.

Technology innovation and an unrelenting push toward a digital world open us up to a range of cybersecurity risks. For retirement plans, it's the risk of sharing financial and personal identifiable information across platforms and third-party service providers. And with participant assets and retirement security on the line, the risks weigh on many plan sponsors' minds.

Until recently, guidance from the Department of Labor (DOL) on the topic has been scarce. In April, the DOL released an article to assist plan sponsors in meeting their fiduciary obligations. To fulfill these duties, plan sponsors are following some simple steps to help protect against a cybersecurity breach. For starters, establishing a well-documented cybersecurity program that includes several critical elements.

Review and Monitor Service Providers

Careful review of service-provider agreements and contract terms is an important first step. It is also a good idea for plan sponsors make sure they understand provider security practices and cybersecurity standards. Plan sponsors will want to explore past security incidents, legal proceedings related to the vendor's services, and the provider's response. Plan sponsors should also verify service providers' insurance policies for cybersecurity and identity theft breaches.

Protect Plan Data

While recordkeepers and other service providers have an obligation to keep private information private, plan sponsors sometimes volunteer more information than required. For example, oversharing

Social Security numbers can open the door for potential misuse. So, while it's necessary to provide participant information for certain purposes, less is generally more.

Insure Against Breaches

Two types of insurance address cyberbreaches: cybersecurity insurance and fiduciary liability insurance. Most employers have a cybersecurity insurance policy covering the organization, but plan sponsors should make sure the policy specifically covers the retirement plan.

Fiduciary liability insurance protects against claims of a breach, but employers and plan sponsors should ensure the policy also covers claims of fiduciary breach due to cybertheft. This specific coverage may require a rider or separate policy.

An indemnification provision in service provider agreements is an added layer of protection. It requires the service provider make a participant whole in the event of a data or dollars breach on the provider's end. The provision ensures the organization is not held financially responsible, nor is an insurance claim needed. Keep in mind, if a contract contains this provision, the plan sponsor must take certain steps to prevent data breaches on their end.

Focus on Participants

Recordkeepers maintain safeguards to ensure the security of participant accounts, but individuals who have never logged in remain vulnerable. In fact, participants rarely log in are less likely to change their passwords or notice any unusual account activity. Meanwhile, participants who have never logged in fail to establish user identification, passwords, and authentication methods to verify identity.

Plan sponsors and recordkeepers should communicate the benefits of logging in on a regular basis. This is not only from a cybersecurity perspective, but also to better understand their path to retirement security. The DOL suggests participants close or delete unused accounts, use caution when accessing unsecured Wi-Fi networks, and be wary of phishing messages asking for personal information.

Maintaining current participant contact information is another way to protect against cyberthreats. However, if contact information is out of date, this safeguard fails. With an ever-increasing digital environment and heightened focus on safety of participants' assets, cybersecurity in retirement plans will remain a DOL focus for years to come. Prudent plan sponsors will take appropriate actions to protect their retirement plans participants and organizations.

Author(s)

Michael A. Webb, CEBS

https://www.captrust.com/people/michael-a-webb-cebs/

Legal Notice