



Cybersecurity: Retirement Plan Sponsors Can Protect Themselves

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

In April 2022, the Department of Labor released an [article](#) to assist plan sponsors in meeting their fiduciary obligations regarding cybersecurity. To fulfill these duties, plan sponsors are following some simple steps that help protect against potential breaches. One place to start is establishing a well-documented cybersecurity program that includes several critical elements, including the four pillars below.

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 to make sure they understand service-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 is required. For



example, oversharing Social Security numbers can open the door to potential misuse. While it is necessary to provide participant information for certain purposes, generally, less is more.

Insure Against Breaches

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

Fiduciary liability insurance protects against claims of a breach, but employers and plan sponsors should ensure that 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 to make a participant whole in the event of a data breach or dollars breach on the provider's end. This type of 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 who 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 practice is not important only to ensure cybersecurity but also to help participants better understand their path to retirement security. The DOL suggests participants close or delete all unused accounts, use caution when accessing unsecured Wi-Fi networks, and be wary of phishing messages that ask for personal information.

Maintaining current contact information for each participant 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 the safety of participants' assets, cybersecurity in retirement plans will remain a DOL focus. Prudent plan sponsors will take appropriate actions now to protect their retirement plan participants and organizations.



Legal Notice

This material is intended to be informational only and does not constitute legal, accounting, or tax advice. Please consult the appropriate legal, accounting, or tax advisor if you require such advice. The opinions expressed in this report are subject to change without notice. This material has been prepared or is distributed solely for informational purposes. It may not apply to all investors or all situations and is not a solicitation or an offer to buy any security or instrument or to participate in any trading strategy. The information and statistics in this report are from sources believed to be reliable but are not guaranteed by CAPTRUST Financial Advisors to be accurate or complete. All publication rights reserved. None of the material in this publication may be reproduced in any form without the express written permission of CAPTRUST: 919.870.6822.

© 2025 CAPTRUST Financial Advisors