Barley Snyder

New DOL Guidance on Cybersecurity and Retirement Plans

PUBLISHED ON
April 19, 2021

$9 trillion.

That's how much the U.S. Department of Labor estimates retirement plans hold in this country, making them a prized target for cybersecurity threats. In addition to plan assets, retirement plans also possess an extensive amount of sensitive personal data. In an effort to assist plan sponsors and third-party administrators with this significant and rapidly growing concern, the department has, for first time, provided guidance addressing cybersecurity.

As an ERISA fiduciary, a plan sponsor should be taking steps to protect plan participants and beneficiaries from cyber thieves. Moreover, when selecting plan service providers, a plan sponsor should carefully assess their cybersecurity preparedness. This guidance offers some insight into what is considered the best practices for plan fiduciaries and third party administrators, and it's fair to say that you should anticipate that future DOL plan audits will include a cybersecurity component.

The much anticipated guidance is available at the department website in the form of Cybersecurity Program Best Practices, Tips for Hiring a Service Provider with Strong Cybersecurity Practices and Online Security Tips for Participants and Beneficiaries.

Under the Cybersecurity Program Best Practices, the department offers a list of 12 best practices, including:

- Perform an annual risk assessment
- Establish a written cybersecurity program
- Provide cybersecurity training
- Ensure that sensitive data is encrypted
- For assets and data stored by outside parties confirm appropriate security reviews and access control procedures

The prudent selection of plan service providers has always been a priority for plan sponsors and with the release of the Tips for Hiring a Service Provider with Strong Cybersecurity Practices, the department offers valuable insight on key cybersecurity considerations when engaging in the selection process, including:

- The service provider's cybersecurity practices and policies as compared to industry standards
- The internal controls and audit process for validating its practices and procedures, security standards implemented, and the availability of external auditor results
- The extent of the service provider's insurance policies for losses related to cybersecurity breaches
- Prover service contract provisions addressing cybersecurity compliance and standard of care to protect

confidential data

- Their track record in terms of past security incidents and legal proceedings

Finally, the DOL also suggests Online Security Tips for Participants and Beneficiaries, such as diligently monitoring accounts, strengthening passwords and paying special attention to common phishing tools.

If you have questions about these developments or other matters involving employer-provided retirement plans, please reach out to me or another member of the firm's Employee Benefits Practice Group or Cybersecurity Service Team.

:

Mark A. Smith

Partner

Tel: (717) 399-1526

Email: msmith@barley.com