WINSTON & STRAWN LLP

BLOG

New Cybersecurity Guidance Applicable to Employee Benefit Plan Contracting

APRIL 20, 2021

Many issues keep employee benefit plan administrators, committees, and sponsors (plan fiduciaries) awake at night, but cybersecurity is especially troubling for many reasons. Employee benefit plans face significant cybersecurity threats and, given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating. Further, plan fiduciaries can have the best cybersecurity procedures in place for their own internal systems, and yet the plan or a plan participant can still experience a cyber-breach because of the numerous interfaces the plan has with third parties, such as record-keepers, custodians, and payroll providers.

Plan fiduciaries have struggled with the question of whether their employee benefit plans' security measures are adequate. In past years, the United States Department of Labor's (DOL) ERISA Advisory Council has examined cybersecurity for employee benefit plans, but failed to issue guidance on the topic. On April 14, 2021, the DOL published guidance for plan fiduciaries, record-keepers, and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers. Although plan fiduciaries can use this guidance for other valuable purposes, this Alert will focus only on the portion of the guidance issued for plan fiduciaries with respect to their service provider contracts.

Most plan fiduciaries rely on service providers to perform the many tasks necessary for establishing and maintaining compliant benefit plans. When engaging new service providers, or monitoring existing service providers and confirming they remain the prudent choice, most plan fiduciaries will conduct a request for proposal (RFP). Service providers who are interested in performing the requested services will participate in that RFP.

Among other important requirements and obligations, a plan fiduciary should include in the RFP cybersecurity questions and representations that a service provider must respond to/agree to make in order to be considered for the engagement. Specifically, the plan fiduciary should:

- Incorporate the DOL's Tips For Hiring A Service Provider With Strong Cybersecurity Practices as a component of that RFP; and
- Require the service provider to represent that it complies, and will comply for the duration of the contract, with the DOL's Cybersecurity Program Best Practices.

Existing service providers may be operating under longstanding contracts that do not address cybersecurity practices. Plan fiduciaries should revisit those service provider agreements and their service provider monitoring process to ensure the above tips and best practices are included in those existing agreements.

In addition to the above, this new cybersecurity guidance gives plan fiduciaries helpful information to include when performing their ongoing governance obligations, including assessing their bonding and insurance needs. If you need assistance, please contact a member of the Winston & Strawn Employee Benefits and Executive Compensation Practice Group or your Winston relationship attorney for further information.

2 Min Read

Authors

Joe Adams

Anne Becker

Amy Gordon

Related Locations

Chicago

Related Topics

Cyber Security

Related Capabilities

Labor & Employment

Privacy & Data Security

Employee Benefits & Executive Compensation

Health Care

Related Regions

North America

Related Professionals

Joe Adams

Anne Becker

Amy Gordon

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.