Patterson Belknap

Employee Benefits and Executive Compensation Alert
October 7, 2024

DOL Updates and Confirms Cybersecurity Guidance Applies to All ERISA Plans

In September 2024, the U.S. Department of Labor (the "DOL") released Compliance Assistance Release No. 2024-01 and its updated cybersecurity guidance for employers that sponsor employee benefit plans governed by the Employee Retirement Income Security Act of 1974, as amended ("ERISA"). Among other things, the DOL clarified that its cybersecurity guidance applies not only to ERISA retirement benefit plans, but also to ERISA welfare benefit plans (such as group health plans).

Background

The DOL originally released its three-part cybersecurity guidance in April 2021, which was intended to "help plan sponsors, fiduciaries, service providers, and participants in employee benefit plans safeguard plan data, personal information, and plan assets." The original 2021 guidance was framed for ERISA retirement plans, leading certain health and welfare plan service providers (e.g., recordkeepers, third-party administrators, etc.) to believe that the 2021 guidance only applied to retirement plans. However, in light of the DOL's increasing prioritization of cybersecurity and growing awareness of the general perception that the 2021 guidance was limited in application, the DOL has now clarified that this is not the case. Because cybercrime, identity theft, and computer-related risks threaten all ERISA-covered plans (including health and welfare benefit plans, which often have sensitive personal participant information), the DOL's cybersecurity guidance now specifically applies to all ERISA-covered plans, including health and welfare benefit plans.

Updated Cybersecurity Guidance

The updated guidance released by the DOL maintains its original three-part format, and continues to direct guidance toward plan sponsors, fiduciaries, and service providers, as well as plan participants:

i. **Tips for Hiring a Service Provider with Strong Security Practices**. This part of the guidance provides six tips to help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires. The guidance suggests specific questions to be raised with service providers, such as requesting details regarding: (a) any past security breaches; (b) information security standards, practices and policies, and audit results; (c) how the service provider validates its security practices; and (d) whether the service provider maintains insurance that covers breaches and cybersecurity losses. The guidance also suggests reviewing public records regarding the service provider's past performance with respect to security incidents and imposing contractual obligations on service providers to ensure ongoing compliance with cybersecurity and information security standards.

ii. **Cybersecurity Program Best Practices**. This part of the guidance holistically sets forth the DOL's expectations for a robust cybersecurity infrastructure used for ERISA-covered plans. This guidance provides twelve detailed best practices to further assist fiduciaries in making prudent hiring decisions with respect to their service providers, and to assist record-keepers and other related service providers in managing internal and external cybersecurity risks, and ultimately better safeguard plan assets, plan data, and personal information (including personally identifiable information and protected health information).

iii. **Online Security Tips**. This part of the guidance suggests that plan participants proactively register for online accounts associated with their retirement accounts or other employee benefit plan information to secure their online identities and provides other basic online best practices to further reduce the risk of fraud and loss (for example, using strong passwords

and multi-factor authentication, keeping personal contact information up to date, avoiding free Wi-Fi, and being mindful of phishing attacks).

Takeaways

The latest guidance from the DOL reminds plan sponsors that ERISA fiduciaries are required to act prudently and in the best interests of plan participants and beneficiaries by taking appropriate precautions to mitigate constantly evolving cybersecurity risks, particularly when selecting and contracting with third-party service providers. In general, in following the DOL's guidance with respect to such service providers, plan sponsors and fiduciaries should:

- request and review the service provider's information and documentation regarding cybersecurity policies, procedures, guidelines, and standards, including results of third-party audits, corrections, and prior breaches;
- include cybersecurity and data privacy provisions in service provider agreements (including, where appropriate, provisions relating to confidentiality of data, notification of breaches, records retention, indemnification, etc.); and
- inquire whether third-party service providers have applicable insurance policies.

Additionally, plan sponsors and fiduciaries may also consider: (a) implementing cybersecurity education or training directed to plan participants; and (b) identifying positions or people within the organization who may provide appropriate cybersecurity expertise and knowledge for selecting and monitoring third-party service providers, establishing security policies, procedures, and controls, conducting ongoing threat monitoring and periodic risk assessments, managing storage and transmission of sensitive data, and incident response and recovery.

This alert is for general informational purposes only and should not be construed as specific legal advice. If you would like more information about this alert, please contact one of the following attorneys or call your regular Patterson contact.

Douglas L. Tang	212.336.2844	dtang@pbwt.com
Jessica S. Carter	212.336.2885	jcarter@pbwt.com
JoAnn Kim	212.336.2221	jokim@pbwt.com

To subscribe to any of our publications, call us at 212.336.2000, email mktg@pbwt.com or sign up on our website, https://www.pbwt.com/subscribe/.

This publication may constitute attorney advertising in some jurisdictions.
© 2024 Patterson Belknap Webb & Tyler LLP

Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, NY 10036–6710
212.336.2000
www.pbwt.com