HILL WARD HENDERSON

DOL RELEASES CYBERSECURITY GUIDANCE FOR RETIREMENT PLANS

Last month, the Department of Labor (DOL) released guidance on cybersecurity for plan sponsors and fiduciaries of qualified retirement plans. This new guidance recognizes that participants and assets of retirement plans are increasingly at risk from internal and external cybersecurity threats, and acknowledges that, as part of their fiduciary duties under ERISA, plan fiduciaries must take appropriate precautions to mitigate such cybersecurity risks.

This new guidance is structured as a series of tips and best practices for plan sponsors, plan fiduciaries, record keepers and plan participants. However, recent commentary from the DOL indicates that how parties address cybersecurity risks will be a part of DOL plan investigation. Based on our experience with recent DOL plan investigations, this is already happening. Therefore, plan fiduciaries should implement practices to ensure that proper cybersecurity protocols are in place, both at the plan fiduciary and service provider level.

This newsletter is meant to summarize the DOL release regarding the guidance, which can be found in its entirety here.

Tips for Hiring a Service Provider

Plan sponsors rely heavily on other service providers to securely maintain plan records and confidential participant data. As part of its fiduciary obligations, plan sponsors must ensure they are engaging and using service providers who follow strong cybersecurity practices. The DOL guidance includes the following tips for plan sponsors to consider in hiring a service provider. Plan sponsors should also consider reviewing existing relationships in light of these tips:

- Ask about the service provider's information security standards, practices and policies, and audit results (including how it validates such practices and what security standards it has met). Compare the provider's practices to the industry standards.
- Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation and legal proceedings related to the service provider's services.
- Ask the service provider whether the service provider has experienced past security breaches and how the service provider responded.
- Inquire whether the service provider has any insurance policies that cover losses caused by cybersecurity and identity theft breaches (both external and internal).
- Review contract provisions with plan service providers regarding cybersecurity to determine what rights are provided to you (e.g., rights to review audit results and other ongoing compliance matters). The guidance also include cybersecurity related terms and provisions that a plan sponsor should attempt to include in its agreements with service providers.

Cybersecurity Program Best Practices for Service Providers

The DOL guidance also provides the following best practices for use by service providers. While directed at service providers, plan sponsors may also use these best practices as a checklist when reviewing and selecting service providers. These best practices for service providers include:

- Having a formal, well documented cybersecurity program.

- Conducting prudent annual risk assessments.
- Having a reliable annual third-party audit of security controls.
- Clearly defining and assigning information security roles and responsibilities.
- Having strong access control procedures.
- Ensuring that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
- Conducting periodic cybersecurity awareness training.
- Implementing and managing a secure system development life cycle (SDLC) program.
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypting sensitive data, stored and in transit.
- Implementing strong technical controls in accordance with best security practices.
- Appropriately responding to any past cybersecurity incidents.

Online Security Tips for Plan Participants

Finally, the DOL guidance provides a number of tips to plan participants to reduce the risk of fraud and loss to their retirement accounts. Plan sponsors should consider providing these security tips to plan participants (separately or as part of existing plan disclosures), or otherwise making participants aware of them as part of the plan sponsor's cybersecurity efforts.

If you have any questions or would like additional information, please contact a member of our Employee Benefits & Executive Compensation Team below.

Al Ward
al.ward@hwhlaw.com
813.222.8703

Kirsten Vignec
kirsten.vignec@hwhlaw.com
813.222.8731

Bret Hamlin
bret.hamlin@hwhlaw.com
813.222.8717

Tim Zehnder
timothy.zehnder@hwhlaw.com
813.222.3113

HILL WARD HENDERSON