DEPARTMENT OF LABOR PUBLISHES CYBERSECURITY GUIDANCE

Hodgson Russ Employee Benefits Newsletter
May 26, 2021

In April, the Department of Labor's ("DOL") Employee Benefits Security Administration ("EBSA"), for the first time, published subregulatory guidance aimed directly at sponsors of ERISA employee benefit plans, ERISA plan fiduciaries, recordkeepers and plan participants that addresses cybersecurity practices. While the EBSA release announcing the guidance draws particular attention to ERISA retirement plans, which hold estimated plan assets of $9.3 trillion, there is nothing in the guidance that limits the application of the guidance to ERISA retirement plans alone. It is not just the trillions of dollars plan assets that merit greater protection from cybersecurity risks, participants' personal information (names, birth dates, Social Security numbers, etc.) also needs protection from increased threats of unauthorized access. Accordingly, ERISA welfare benefit plans would be well served by also implementing the relevant cybersecurity practices described in the new guidance.

EBSA's cybersecurity guidance takes the form of three separately published documents:

• Tips for Hiring a Service Provider, which offers plan sponsors and fiduciaries tips for prudently selecting and monitoring service providers with strong cybersecurity practices.

• Cybersecurity Program Best Practices, which assists plan fiduciaries and recordkeepers in meeting their responsibilities to manage cybersecurity risks.

• Online Security Tips, which offers plan participants and beneficiaries tips on how they can reduce the risk of fraud and loss to their retirement account when checking their retirement accounts online.

Although the DOL, via EBSA or otherwise, has not previously provided specific cybersecurity guidance for ERISA employee benefit plans, there have been increasing indirect indicators of the DOL's growing concerns about cybersecurity threats to plan assets and personal information. Plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks. The new guidance not only offers helpful insights on what practices and procedures EBSA would consider important to prudently mitigate cybersecurity risks, but it suggests standards of cybersecurity practices we might expect EBSA to look for in future audits and investigations.

Attorneys

Peter Bradley
Michael Flanagan
Richard Kaiser
Ryan Murphy
Amy Walters

Practices & Industries

Employee Benefits

The amplified focus on cybersecurity not only pertains to a plan sponsor's own internal administrative procedures, but also to the cybersecurity practices and procedures of recordkeepers and other service providers that plan sponsors select to support ERISA plan operations. Are plan sponsors asking the right questions of recordkeepers and service providers regarding their information security standards, practices and policies, and are adequate protections built into service agreements? The new guidance provides suggested lines of questioning that plan sponsors of all sizes should be asking as part of their selection and monitoring process for their service providers.

Best practices for plan service providers should 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 respond to any past cybersecurity incidents.

The fact that the new EBSA guidance includes online security tips for plan participants reflects a recognition that participants have their own role to play in reducing the risk of fraud and loss with respect to their individual retirement accounts. Plan sponsors will want to consider making those online security tips part of the standard plan enrollment and communication packages that go to participants.

In light of the new guidance, plan sponsors should be looking to develop appropriate internal cybersecurity practices and policies (including hiring practices and policies for new plan service providers), or to update any such practices and policies that are already in place. For existing service providers, a review of provider cybersecurity practices, policies and contractual responsibilities (i.e., service agreement provisions), as well as the development of appropriate mechanisms for monitoring cybersecurity practices going forward, is advisable.