Insights

U.S. Department of Labor Issues Cybersecurity Guidance for Retirement Plans

July 13, 2021

By: Lisa A. Durham

Cybersecurity threats are becoming ubiquitous in today's technology-driven, cloud-based society and even more so now as the COVID-19 pandemic has fundamentally changed the way people work, communicate, and save. No information is safe and no financial assets, including your 401(k) plan, are invulnerable to being penetrated by sophisticated and highly motived cybersecurity thieves. However, the U.S. Department of Labor (the "DOL") is taking notice.

This past April, the DOL, through its Employee Benefits Security Administration ("EBSA") department, issued cybersecurity guidance for the first time for plan sponsors, plan fiduciaries, record keepers and plan participants. The guidance, in addition to seeking to protect an estimated $9.3 trillion in assets that are in plans that are regulated by the Employee Retirement Income Security Act ("ERISA"), aims at assisting plan sponsors and fiduciaries but also provides valuable information for plan participants and beneficiaries as well. The news release and substantive guidance from the DOL can be found **here**.

The DOL's guidance comes in three parts: (1) Tips for Hiring a Service Provider; (2) Cybersecurity Program Best Practices; and (3) Online Security Tips.

Tips for Hiring a Service Provider

As part of the process of sponsoring a 401(k) or other type of pension plan, employers and business owners typically choose and rely on a service provider to maintain plan records and keep plan and participant data confidential. In this portion of the guidance, EBSA provides tips and best practices to plan sponsors and fiduciaries to ensure that they are discharging their duties properly under ERISA when choosing a service provider.

This includes but is not limited to: (1) asking about and evaluating a service provider's track record of cybersecurity incidents, (2) investigating whether a servicer provider has adequate insurance coverage to cover losses caused by cybersecurity, and (3) drafting a service provider contract that (i) ensures routine information security reporting, (ii) obligates service providers to notify plan sponsors of cybersecurity breaches, and (iii) complies with all applicable federal, state, and local laws that relate to privacy, confidentiality, or security of plan participant's personal information.

Cybersecurity Program Best Practices

Under ERISA, plan fiduciaries have an obligation to mitigate risks associated with cybersecurity. In this portion of the guidance, EBSA provides best practices to recordkeepers and other service providers for meeting and discharging their responsibilities to manage and mitigate cybersecurity risks.

Best practices include but are not limited to: (1) drafting a formal, well documented cybersecurity program; (2) annually assessing cybersecurity risks; (3) annually auditing third parties of security controls; and (4) implementing strong access control procedures.

Online Security Tips

This portion of the guidance aims to help both plan participants and beneficiaries from risk of fraud or loss in their retirement accounts. The tips provided can be invaluable for not only managing cybersecurity risks in a retirement account but also managing cybersecurity risks in other online accounts, such as a checking or brokerage account. Tips include: using a strong and unique password, using multi-factor authentication, and routinely monitoring your online account for fraud and theft.

Takeaways

It is critical for plan sponsors, service providers, and plan participants to continue to communicate and be aware of cybersecurity threats to plan assets. Plan sponsors and employers need to ensure that the participants in their plans are using proper passwords and monitoring their retirement accounts on a routine basis. Plan sponsors need to have an extensive vetting process of potential service providers, including reviewing service contracts with cybersecurity threats in mind. If mitigating cybersecurity procedures were not implemented by a plan sponsor, plan fiduciary, or service provider and a cyber theft occurs, fiduciary obligations under ERISA would be breached and lawsuits may be filed.

Cybersecurity threats and breaches are here to stay. It is integral to be aware of these threats and take the right steps forward to mitigate them. If you have any questions regarding your service provider or your service provider contract, your obligations to mitigate cybersecurity threats under ERISA as a plan sponsor, or any other best practices to safeguard financial assets and personal data in retirement accounts, please contact **Lisa A. Durham** or another member of **Krieg DeVault's Employee Benefits Group**.