ERISA Litigation

DOL Issues New Guidance on Cybersecurity for Retirement Benefit Plans

By: Katherine M. Funderburg, Jennifer T. Beach, and Joseph J. Torres

The Department of Labor (DOL) has issued its first-ever guidance[1] on cybersecurity for ERISA-regulated retirement benefit plans. This guidance comes shortly after the Government Accountability Office (GAO) released a report[2] calling on the DOL to clarify how plan administrators should address cybersecurity risks for defined benefit plans. The DOL's guidance, which suggests combating cybercrime should be a priority for plan sponsors and fiduciaries, also provides tips to participants and beneficiaries on how to guard against cyber threats.

The guidance has three parts: one directed at plan sponsors, one directed at record keepers and service providers, and one directed at plan participants.

The guidance for participants includes a number of online security tips aimed at helping workers protect their accounts, which often represent the sole source of retirement savings. The DOL advises workers to routinely monitor their accounts and to use strong passwords and multi-factor authentication.[3] DOL also warns participants against phishing attacks and provides a list of common indicators that a message is a phishing attempt.[4]

DOL's guidance to plan sponsors focuses on tips for hiring third-party service providers with strong cybersecurity practices, emphasizing employers' and fiduciaries' responsibilities to "prudently select and monitor" such service providers.[5] The guidance recommends that plan sponsors understand various aspects of prospective service providers' information security standards and practices—such as results of past audits, responses to prior security breaches, and insurance policies that would cover cyber attack losses—before contracting with them.[6] Plan sponsors are also instructed to ensure that their service providers' contracts require ongoing compliance with cybersecurity and information security standards, and to avoid provisions that limit service providers' responsibility for breaches.[7]

The guidance for record keepers and service providers provides tips for instating policies that protect worker data. DOL notes that retirement plans may be targeted for cyber attacks because they often hold millions of dollars in assets and include participants' personal data.[8] Accordingly, DOL states, "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."[9] DOL sets out 12 best practices for fiduciaries, record keepers, and other service providers, who are advised to:

- Have a formal, well documented cybersecurity program;[10]
- Conduct annual risk assessments;[11]
- Have a reliable annual third-party audit of security controls;[12]
- Clearly define and assign information security roles and responsibilities;[13]
- Have strong access control procedures;[14]

- Ensure that 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;[15]
- Conduct periodic cybersecurity awareness training;[16]
- Implement and manage a secure system development life cycle program;[17]
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response;[18]
- Encrypt sensitive data, stored and in transit;[19]
- Implement strong technical controls in accordance with best security practices;[20] and
- Appropriately respond to any cybersecurity incidents.[21]

DOL also provides recommendations on how to implement each of these best practices.[22]

Many of these cybersecurity practices are already commonplace; however, it is likely that going forward, compliance with these practices will be cited in ERISA litigation as relevant standards against which a plan's data security should be measured. Plan sponsors and fiduciaries should evaluate these recommendations and consider the extent to which they should be incorporated into any relevant plan documents or contracts.

Contact Us

Katherine M. Funderburg
kfunderburg@jenner.com | Download V-Card

Jennifer T. Beach
jbeach@jenner.com | Download V-Card

Joseph J. Torres
jtorres@jenner.com | Download V-Card

Meet Our Team

Practice Leader

Joseph J. Torres

Chair

jtorres@jenner.com

Download V-Card

---

[1] D.O.L. News Release 21-358-NAT (Apr. 14, 2021), https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.

[2] GAO-21-25, *Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans (2021)*, https://www.gao.gov/products/gao-21-25.

For further discussion of the GAO report, please see our prior publication, *GAO Report Calls for DOL Guidance on Cybersecurity Obligations for Defined Contribution Plans* (Apr. 14, 2021), https://jenner.com/library/publications/20907.

[3] *Online Security Tips*, Employee Benefits Security Administration, at 1 (Apr. 14, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

[4] *Id.* at 1–2.

[5] *Tips for Hiring a Service Provider with Strong Cybersecurity Practices*, Employee Benefits Security Administration, at 1 (Apr. 14, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf.

[6] *Id.*

[7] *Id.*

[8] *Cybersecurity Program Best Practices*, Employee Benefits Security Administration, at 1 (Apr. 14, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

[9] *Id.*

[10] *Id.* at 1–2.

[11] *Id.* at 2.

[12] *Id.*

[13] *Id.* at 3.

[14] *Id.*

[15] *Id.* at 3–4.

[16] *Id.* at 4.

[17] *Id.*

[18] *Id.* at 4–5.

[19] *Id.* at 5.

[20] *Id.*

[21] *Id.*

[22] Plan sponsors, record keepers, and service providers should also be aware of existing Employee Benefits Security Administration (EBSA) regulations that govern the use of electronic media for maintenance and retention of records. *See* 29 C.F.R. § 2520.107-1.