A SUMMARY:
DOL Issues Cybersecurity Guidance

EXPERIENTIAL WEALTH
FIDUCIA PERPETUA

On April 4, 2021, the Employee Benefits Security Administration of the Department of Labor issued a new guidance for plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act (ERISA). The guidance offers tips and the Department of Labor's view of "best practices" in three areas:

- **Tips for Hiring a Service Provider**[1]
- **Cybersecurity Program Best Practices**[2]
- **Online Security Tips**[3]

Although the Tips and Best Practices are not formal, binding guidance, they can definitely serve as baseline information for plan fiduciaries when selecting and monitoring service providers. Since not every fiduciary or plan sponsor has cybersecurity and privacy law expertise, working with experts can be helpful. Further, plan fiduciaries can benefit from reviewing these Tips and Best Practices in light of their current and future service providers.

The DOL's suggestions include:

Tips for Hiring a Service Provider

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.
2. Ask the service provider how it validates its practices and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.
3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors and

[1] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf
[2] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf
[3] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf

breaches caused by external threats, such as a third party hijacking a plan participants' account).

6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants.

Cybersecurity Program Best Practices

The following best practices are for use by recordkeepers and other service providers responsible for plan-related IT systems and data and for plan fiduciaries making decisions on the service providers they should hire. Per the DOL, the Plans' service providers can look to consider:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third-party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure 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.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Respond appropriately to any past cybersecurity incidents.

Online Security Tips

The Tips are a fairly standard list of to-dos, and plan fiduciaries may find it helpful to notify all employees of these prophylactic action steps:

1. Register, set up and routinely monitor your online account.
2. Use strong and unique passwords.
3. Use multi-factor authentication.
4. Keep personal contact information current.
5. Close or delete unused accounts.

6. Be wary of free wi-fi.
7. Beware of phishing attacks.
8. Use antivirus software and keep apps and software current.
9. Know how to report identity theft and cybersecurity incidents[4].

ERISA plan fiduciaries are required to serve solely in the interest of plan participants and beneficiaries with loyalty and due care. EBSA's publication of these best practices to follow regarding cybersecurity, highlight the importance of evaluating cybersecurity and privacy practices. Plan fiduciaries have an ongoing duty to monitor their service providers, and now, plan sponsors have a clearer understanding of EBSA's recommended steps regarding cybersecurity.

https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414

This summary, prepared by Philip Chao, is for general informational purpose only and should not be deemed as delivering any legal or regulatory guidance or advice regarding the subject matter. Please refer to EBSA News Release in its entirety for a more complete understanding and application. Please consult with legal and regulatory counsel before taking any action. This Firm is not a cybersecurity or IT expert and is not in the business of delivering advice on such matters.

[4] https://www.cisa.gov/reporting-cyber-incidents
https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view