Cybersecurity and a Plan Sponsor's FIDUCIARY DUTY

STRATEGIC RETIREMENT PARTNERS

The Employee Retirement Income Security Act of 1974 (ERISA) was enacted in a time when cybersecurity was not in the dictionary. Over the past 10 years, cybertheft has exploded into a major and growing issue for protecting American's financial assets including retirement accounts. ERISA has not been amended or interpreted to impose a specific duty on plan fiduciaries to maintain appropriate cybersecurity protections. However, that does not mean plan fiduciaries do not have a responsibility to address the issue on behalf of participants[i]. The duties of prudence and loyalty are being challenged in several court cases and may be interpreted to include a responsibility to keep plan assets safe from hackers.

Department of Labor Issues Cybersecurity Guidance

In April 2021, the Department of Labor (DoL) Employee Benefits Security Administration (EBSA) provided guidance[ii] for plan sponsors, plan fiduciaries, recordkeepers and plan participants regarding cybersecurity. The guidance included three resources:

- **Tips for hiring a Service Provider[iii]:** Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.
- **Cybersecurity Program Best Practices[iv]:** Assist plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks.
- **Online Security Tips[v]:** Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

Acting Assistant Secretary for the EBSA, Ali Khawar, hailed the guidance as "an important step towards helping plan sponsors, fiduciaries and participants to safeguard retirement benefits and personal information." Khawar added, "This much-needed guidance emphasizes the importance that plan sponsors and fiduciaries must place on combatting cybercrime."[vi]

Plan Sponsor Fiduciary Responsibilities

Fiduciaries have a duty of loyalty to plan participants and must execute their duties solely in the interest of plan participants and beneficiaries. A failure to evaluate and monitor the cybersecurity protocols of service providers and their ability to keep participants secure could potentially violate this duty.

Prior to the DoL issuing guidance in April of 2021, the most widely referenced ERISA regulations referencing a plan sponsor's duty regarding cybersecurity was in participant disclosure regulations and stated the following:

> "[A]ppropriate and necessary measures reasonably calculated to ensure that the system for furnishing documents … protects the confidentiality of personal information relating to the individual's accounts and benefits (e.g., incorporating into the system measures designed to preclude unauthorized receipt of or access to such information by individuals other than the individual for whom the information is intended)." (ERISA Reg. Section 2520.104b1(c)(1)(i))

With this additional DoL guidance and the exponential increase in cybercrime[vii], it is more important than ever for plan sponsors to make cybersecurity review of vendors, particularly recordkeepers, a priority in their due diligence process.

Service Providers and Plan Sponsors Named in Recent Cybersecurity Lawsuits Including:

- American Trust (Third Party Administrator (TPA)), February 2020[viii] – Participant balance of $124,105 stolen.
- Alight Solutions LLC (recordkeeper) and Abbot Laboratories (plan sponsor), April 2020[ix] – Participant balance of $245,000 stolen.
- Nationwide Trust (recordkeeper) and MandMarblestone Group LLC (TPA), October 2020[x] – Participant balance of $400,000 stolen.
- Alight Solutions LLC (recordkeeper) and Estée Lauder Inc (plan sponsor) November 2019[xi] – Participant balance of $99,000 stolen.

The DOL Offers Tips to be used as Best Practices for Plan Fiduciaries

Plan fiduciaries should inquire about their service provider's compliance with the EBSA best practices for recordkeepers and other service providers[4] and document their process. Working with an advisor who can offer assistance with this process and specializes in retirement plan consulting may be an additional service to bring value to a plan sponsor. The DoL tips include[xii]:

- **Request information from service providers including:**
    - Audit type and results, information security standards, practices and policies.
    - How practices are validated
    - What levels of security standards it has met and implemented
    - Whether the service provider has experienced past security breaches, what happened, and how the service provider responded,
- **Evaluate service providers based on the following:**
    - Do they follow a recognized standard for information security and use an outside auditor to review and validate cybersecurity?
    - Are there contract provisions that give you the right to review audit results demonstrating compliance with security standards?
    - How does the service provider's standards compare to competitors in the industry?
    - What is the service provider's track record in the industry, including public information regarding information security incidents, other litigation and legal proceedings related to its services?
    - Are there any insurance policies that would cover losses caused by cybersecurity and identity theft breaches?
    - Does the service contract require ongoing compliance with cybersecurity and information security standards?

- **Best in Class Service Providers will offer the following:**
    - Information Security Reporting including a third party audit such as a SOC 2, Type II audit or comparable.
    - Clear Provisions on the Use and Sharing of Information and Confidentiality.
    - Notification of Cybersecurity Breaches.
    - Compliance with Laws Concerning Records Retention and Destruction, Privacy and Information Security.
    - Insurance such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage.

What are SOC Audits?

- **SOC** stands for System and Organization Controls through which a CPA reports on an organizations' enterprise-wide cybersecurity risk management program.
- **SOC 1** report evaluates internal controls, policies, and procedures as it relates to the effect of the controls on the vendor's financial reporting.
    - SOC 1 report addresses only internal controls over financial reporting; it does not address broader entity cybersecurity controls and risk.
- **SOC 2** reports on controls that directly relate to the security, availability, processing integrity, confidentiality, and privacy at a service organization. SOC 2 report includes substantial detail specifically related to which controls are in place at the service organization as well as how those controls were tested by the auditor.
    - A SOC 2 report is specifically designed to address controls at a service organization relevant to the systems at the service organization used to process users' data.
- **SOC 3** report is a general use report that can be distributed to any party or parties. In addition, the report is much smaller in size (compared to a SOC 2) and consists of a brief auditor's opinion, management assertion, and a brief narrative providing background on the service organization.
- **NOTE on SOC 2 vs SOC 3:** The audit work that is performed for both SOC 2 and SOC 3 is essentially the same since both examinations are reporting on the company's internal controls specific to the Trust Service Principles with the only differences being the structure of the two reports.
- **Type I** report is an attestation of controls at a service organization at a specific point in time.
- **Type II** report is an attestation of controls at a service organization over a minimum six-month period.
- **AICPA SOC for Cybersecurity** is a new risk framework (2017) that establishes common criteria and guidelines for communicating about an organization's cybersecurity risk management program. It enables plan management to report on the plan's cybersecurity management program to external stakeholders with an independent examination report.

- **SOC for Cybersecurity** is not yet a widely conducted audit but may grow in popularity with the new DoL guidelines.

About the Author

Connect with Erin Hall on LinkedIn

Erin Hall, MBA, AIF, C(k)P, CPFA
Managing Director, Los Angeles
erinh@srpretire.com
Ph: 866.SRP.401K x 762
srpretire.com/who-we-are/team/ehall/

---

[i] https://www.jdsupra.com/legalnews/new-cybersecurity-decision-highlights-47636/
[ii] https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414
[iii] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf
[iv] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf
[v] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf
[vi] https://www.napa-net.org/news-info/daily-news/dol-unveils-cybersecurity-guidance-recordkeepers-fiduciaries?utm_source=MagnetMail&utm_medium=email&utm_term=erico@srpretire.com&utm_content=COM%5FNAPA%5FeNews%5F04%2E15%2E2021%5FDaily%5FThurs&utm_campaign=What%20a%20Difference%20a%20Year%20Makes%20for%20401%28k%29%20Participant%20Traders
[vii] https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
[viii] https://www.planadviser.com/retirement-plan-trustee-faces-cybersecurity-related-lawsuit/
[ix] https://www.groom.com/resources/new-lawsuit-alleges-fiduciary-breaches-by-plan-sponsor-and-recordkeeper-for-quarter-million-dollar-cybertheft/
[x] https://hallbenefitslaw.com/recent-cybersecurity-breach-case-proves-risks-are-rife-for-both-retirement-plan-sponsors-and-service-providers/
[xi] https://securityledger.com/2019/11/suit-against-estee-lauder-spotlights-401k-distribution-fraud/
[xii] https://www.napa-net.org/news-info/daily-news/dol-unveils-cybersecurity-guidance-recordkeepers-fiduciaries?utm_source=MagnetMail&utm_medium=email&utm_term=erico@srpretire.com&utm_content=COM%5FNAPA%5FeNews%5F04%2E15%2E2021%5FDaily%5FThurs&utm_campaign=What%20a%20Difference%20a%20Year%20Makes%20for%20401%28k%29%20Participant%20Traders