TRUCKER ✦ HUSS

DOL Issues New Cybersecurity Guidance — What Plans and Service Providers Need to Know

JENNIFER WONG AND
NICOLAS DEGUINES

APRIL 2021

On April 14, 2021, the Department of Labor's (DOL) Employee Benefit Security Administration (EBSA) issued its first cybersecurity guidance for plan sponsors, plan fiduciaries, recordkeepers, and plan participants.[1] Intended to complement EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries, the guidance is comprised of the following three parts:

- Tips for plan sponsors and fiduciaries to help them prudently hire and monitor service providers;
- Cybersecurity program best practices for plan fiduciaries and recordkeepers that are responsible for maintaining plan-related IT systems; and
- Online security tips for plan participants and beneficiaries who check their retirement accounts online to reduce the risk of fraud and loss.

As the guidance may be considered a "safe harbor" for fiduciaries to show compliance with their obligations under ERISA, plans should take steps now to review the way plan data is protected and revisit contracts with service providers to incorporate the DOL's recommendations accordingly.

What Led to the Guidance

In May 2020, the DOL finalized "safe harbor" regulations to make electronic delivery (e-delivery) of retirement plan updates and notices to participants and beneficiaries the default method of delivery. Under, ERISA, a plan administrator is required to deliver plan information using measures reasonably calculated to ensure actual receipt of the material by plan participants, beneficiaries,

and other individuals.[2] The safe harbor permits plan administrators to email or publish online benefit statements as the default method of delivery, provided participants who prefer printed paper disclosures have the right to opt out.

While the 2020 safe harbor allows plans to take advantage of the innovations and cost savings of electronic communications, there was a recognition that the increased delivery of such information and communications inevitably raises concerns about the heightened cybersecurity risk to participant data.

GAO Report

In February 2021, the Government Accountability Office (GAO) released a report examining (1) the data that plan sponsors and providers exchange during administration of the plan and the associated cybersecurity risks, and (2) efforts to assist plan sponsors and providers to mitigate those risks.[3] The GAO found that within the administration of a plan, plan sponsors and service providers exchange personally identifiable information (PII) and plan asset data, including names, social security numbers, dates of birth, addresses, usernames/passwords, and retirement and bank account numbers. The GAO found that the sensitive nature of the "sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and service providers, as well as plan participants."[4] As a result, the GAO recommended that the DOL (1) formally state whether plan fiduciaries are responsible for mitigating cybersecurity risks, and (2) establish minimum expectations for addressing cybersecurity risks.

DOL Response

In the new cybersecurity guidance, the DOL states that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks," and that the tips provided are meant to "help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers."[5] Although this is not a specific statement extending the fiduciary responsibility to prevent cyberattacks and fraud, the DOL has put plan fiduciaries on notice regarding the expectation to mitigate these cybersecurity risks. The DOL also established minimum expectations for addressing cybersecurity risks. The guidance provides three different sets of recommendations for the different parties involved in the sharing of PII and plan asset information.

Tips for Hiring a Service Provider [6]

To help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, the EBSA recommends the following for evaluating service providers:

- Compare the service provider's security standards to industry standards and review audit results.
- Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.
- Evaluate the service provider's track record in the industry.
- Ask whether the service provider has experienced past security breaches.
- Find out if the service provider has any insurance policies and what is covered.

- Look for contract provisions that require ongoing compliance with cybersecurity standards.
- Beware of contract provisions that limit the service provider's responsibility for IT security breaches.

Cybersecurity Program Best Practices [7]

To assist plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks, EBSA recommends the following:

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

Online Security Tips [8]

To reduce the risk of fraud and loss to plan participants and beneficiaries who check their retirement accounts online, EBSA recommends that plan participants and beneficiaries:

- Register, set up and routinely monitor their online account.
- Use strong and unique passwords.
- Use multi-factor authentication.
- Keep personal contact information current.
- Close or delete unused accounts.
- Be wary of free Wi-Fi.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.

Cybersecurity Litigation

With the increasing risk of cyberattacks, plan administrators have long had concerns regarding whether participant data may be considered a "plan asset" under ERISA and, therefore, whether a breach of such data may constitute a breach of their fiduciary responsibility. Recent cases alleging breach of fiduciary duty have been brought against plan sponsors and administrators for allowing participant accounts to be exposed to fraud, resulting in losses of their entire 401(k) account balance.[9] Claims include failure to implement procedures to safeguard against fraudulent withdrawals, failure to give notice of distributions, and failure to safeguard plan assets. In *Bartnett v. Abbott Laboratories*, the district court declined to extend the fiduciary duty of prudence to require the safeguarding of data and prevention of scams. However, as the DOL's guidance considers the selection and monitoring of service providers with strong cybersecurity practices a task which must be administered prudently — expressly stating that ERISA requires plan fiduciaries to take appropriate precautions to mitigate cybersecurity risks — plans can probably expect to see fiduciary breach claims brought whenever a data security breach event occurs.

Recommendations and Open Issues

Although the DOL guidance is labeled as "best practices" and "tips," plan sponsors and service providers would do well to implement each of the steps recommended in the guidance, including revisiting contracts with service providers to help ensure they have appropriate measures in place to manage cybersecurity risks. As discussed above, plan fiduciaries can be exposed to legal challenges if they fail to meet their fiduciary responsibility to prudently protect retirement benefits. Although the DOL did not specifically require that the guidance must be followed to meet the fiduciary responsibility standard, the DOL has identified these steps as appropriate precautions to mitigate the risk of cyberattacks, which in turn can help limit exposure to liability even in the face of a cyberattack. As the cybersecurity landscape continues to evolve, additional guidance from the DOL would not be surprising. If you have any questions regarding the foregoing, please contact the authors of this article or the Trucker Huss attorney with whom you normally work.

---

[1] https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414

[2] 29 CFR § 2520.104(b)-1(b)(1).

[3] U.S. Government Accountability Office, GAO-21-25, Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(K) and Other Retirement Plans (2021).

[4] *Id.*

[5] Department of Labor, Cybersecurity Best Practices (2021); Department of Labor, Tips for Hiring a Service Provider with Strong Cybersecurity Practices (2021).

[6] Department of Labor, Tips for Hiring a Service Provider with Strong Cybersecurity Practices (2021).

[7] Department of Labor, Cybersecurity Best Practices (2021).

[8] Department of Labor, Online Security Tips (2021).

[9] *See Leventhal v. The MandMarblestone Group LLC*, No. 2:18-cv-02727, 2020 WL 2745740 (E.D. Pa. May 27, 2020), *Berman v. Estee Lauder Inc.*, No. 3:2019-cv-06489 (N.D. Cal. 2019), *Bartnett v. Abbott Laboratories*, No. 1:20-cv-02127, 2020 WL 5878015 (N.D. Ill. Oct. 2, 2020).

EMAIL JENNIFER WONG