Articles + Publications | April 28, 2021

Cybersecurity Security Best Practices for Retirement Plan Administration

WRITTEN BY

James E. Earle | Christopher Stock | Mamta K. Shah

Introduction

The U.S. Department of Labor's (DOL) Employee Benefits Security Administration (EBSA) estimates that there are 34 million defined benefit plan participants in private pension plans and 106 million defined contribution plan participants with combined assets of $9.3 trillion. Participants increasingly access their plan accounts and take actions on their plan benefits through online tools made available by plan sponsors and service providers. In fact, in 2020, the DOL finalized rules encouraging electronic delivery and disclosures of plan information.[1] As a result, it should come as no surprise that participant data and plan assets are increasingly becoming a target of cybercriminals.

On April 14, the EBSA issued guidance for plan sponsors, plan fiduciaries, plan service providers, and plan participants on best practices for maintaining cybersecurity and protecting retirement plan assets (2021 Guidance).[2] The 2021 Guidance is the first formal guidance issued by the EBSA on cybersecurity and builds upon a report by the DOL's ERISA Advisory Council, "Cybersecurity Considerations for Employee Benefits Plans," published in November 2016.[3] The 2021 Guidance does not focus on the cybersecurity of the plan sponsor or the plan fiduciary, but rather the duty of plan fiduciaries for the cybersecurity of plan service providers retained by the plan fiduciaries.

The 2021 Guidance reinforces that ERISA requires plan fiduciaries to take appropriate precautions when engaging and retaining service providers to mitigate the risks posed by cybercriminals and protect plan assets. In this article, we will:

- provide a brief overview of ERISA fiduciary duties to set context for the 2021 Guidance;
- describe the key features of the 2021 Guidance; and
- illustrate the realities of the cybersecurity risk to retirement plans by reviewing a recent case involving cybertheft of a participant's 401(k) account.

ERISA Fiduciary Duties

ERISA requires retirement plan fiduciaries to carry out their duties solely in the interest of plan participants and their beneficiaries and for the exclusive purpose of providing for their benefits (*i.e.,* the duty of loyalty). ERISA also

requires that fiduciaries perform their responsibilities with prudence (*i.e.,* the duty of prudence). To meet the ERISA prudence standard, the fiduciary must act "with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in like capacity and familiar with such matters would use. …" If these duties are breached, ERISA fiduciaries can be personally liable for any resulting plan losses and, in extreme cases involving willful malfeasance, may be criminally liable.

The ERISA concerns regarding cybersecurity generally focus on the duty of prudence, which includes the duty to monitor service providers engaged to assist in plan administration. Whether cybersecurity breaches impacting ERISA plans constitute breaches of fiduciary duties will vary based on the facts and circumstances of the breach, as illustrated in the recent case discussed below, including whether the plan fiduciary has adopted and followed a prudent process in establishing his/her cybersecurity policies.

New DOL Guidance

The 2021 Guidance is comprised of three parts and includes "tips" and "best practices" for plan sponsors, plan fiduciaries, plan service providers, and plan participants.

The first piece of the 2021 Guidance, Tips for Hiring a Service Provider With Strong Cybersecurity Practices, provides much-awaited guidance to plan sponsors and fiduciaries on how to prudently select a service provider with strong cybersecurity practices and procedures. The guidance makes the following recommendations when selecting service providers:

- 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.

- 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.

- Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to the vendor's services.

- Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

- Find out if the service provider has any insurance policies to 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 breaches caused by external threats, such as a third party hijacking plan participants' accounts).

- Make sure that the service provider agreement requires ongoing compliance with cybersecurity and information security standards — and beware of contract provisions that limit the service provider's responsibility for IT security breaches.

PLANNING OPPORTUNITY: This list should form a checklist for plan sponsors and fiduciaries when selecting and periodically reviewing the services provided by plan recordkeepers or other service providers engaged to assist with a retirement plan.

The EBSA also issued Cybersecurity Program Best Practices to provide guidance to plan fiduciaries, recordkeepers, and other service providers regarding their responsibilities for managing cybersecurity risks. Best practices include:

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

PLANNING OPPORTUNITY: If not already doing so, plan sponsors should engage with their internal technology security team to review and consider cybersecurity practices and training related to retirement plan administration.

Even the best policies and procedures can be thwarted if plan participants are not properly educated on the latest security protocols. Recognizing the risk plan participants can create, the EBSA also issued Online Security Tips for plan participants, which include the following tips:

- Register, set up, and routinely monitor online accounts.

- Use strong and unique passwords.
- Use multifactor authentication.
- Keep personal contact information current.
- Close or delete unused accounts.
- Avoid using free Wi-Fi.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.

PLANNING OPPORTUNITY: If not already doing so, plan sponsors should consider cybersecurity training for employees to expressly cover security practices related to retirement plan participation and to understand whether third-party recordkeepers also have cybersecurity training available to participants.

Recent Cybersecurity Case Law: Illustration of Real-Life Cybersecurity Risks

A recent U.S. District Court case illustrates the real-world impact of cybersecurity risks for retirement plans and shows how courts are beginning to approach ERISA fiduciary issues related to cybersecurity breaches. This case underscores the importance of maintaining sound cybersecurity and data protection practices as described in the 2021 Guidance.

In *Bartnett v. Abbott Laboratories, et al*.[4], the plaintiff, a retired former employee of Abbott Laboratories (Abbott Labs) and a 401(k) participant, sued Abbott Labs, an Abbott Labs officer who served as the plan's named fiduciary and administrator, and Alight Solutions LLC (Alight), which served as the plan's recordkeeper and administrator for the plan's website, for alleged breaches of their fiduciary duties under ERISA in failing to prevent the cybertheft of the participant's 401(k) plan account.

The following summarizes the facts as alleged by the plaintiff in her complaint, as described by the court in its opinion. A cybercriminal apparently accessed the plaintiff's 401(k) plan account through the plan's website and added direct deposit information for a different bank account. A few days later, the thief, posing as the plaintiff, called the plan's customer service phone line and told the customer service representative that she tried to process a distribution online but was unsuccessful. Both the website and customer service phoneline were operated by Alight. The service representative responded by reading aloud a home address and asking the thief if she still lived there. The service representative told the thief that the new account must be on file for seven days before money can be transferred from the plan. After the required waiting period, the criminal called the service representative again to request the transfer of $245,000 from the plaintiff's plan account to the new account. The service representative complied without asking any security questions. A day after the transfer, Alight sent a letter to the plaintiff advising her of the transfer. When the plaintiff received the letter, the funds had already been successfully transferred to the new account. As of February 2021, the plaintiff had only recouped about $108,000

of the $245,000 stolen. The plaintiff subsequently filed suit, and the defendants filed a motion to dismiss.

On October 20, 2020, the *Bartnett* court dismissed the claims against Abbott Labs, holding that "the complaint fails to allege any fiduciary acts taken by Abbott Labs, no less link them to the alleged theft." The court also dismissed the allegations against the Abbott Labs officer acting as the plan administrator on similar grounds. The court noted that the theft occurred via the plan's website, which was operated by Alight, not Abbott Labs or the officer acting as the plan administrator. The court found that the complaint failed to allege facts specific enough to show that Abbott Labs failed to monitor Alight's cybersecurity performance as to the plan's website. While the complaint alleged that Alight had experienced other cybersecurity incidents that Abbott Labs should have considered, none were related to the Abbott Labs plan, and most occurred after Abbott Labs had decided to engage Alight.

The court, however, denied Alight's motion to dismiss. The court reasoned that the complaint provided sufficient factual allegations "to infer that Alight acted as a fiduciary by exercising discretionary control or authority over the plan's assets" through its operation of the plan's call center and website that administers distributions, and that the events leading to the theft of the plaintiff's account occurred because of Alight's breach of its duties in operating the website and call center.

Although, the plaintiff could not establish sufficient facts to state a claim against Abbott Labs or its officer acting as the plan administrator, the case certainly emphasizes the importance of plan sponsors and named fiduciaries researching and monitoring the cybersecurity practice and procedures of any third-party plan service providers.

Conclusion

In light of the 2021 Guidance, plan fiduciaries and plan service providers should strongly consider reviewing their cybersecurity policies and processes to ensure such policies and processes conform to the guidance. For plan fiduciaries, the review of service provider cybersecurity processes and policies is not a one-time event. The ERISA duty of prudence not only requires a plan fiduciary to use a prudent process in selecting a plan service provider, but it also requires the fiduciary to continue to monitor the service provider. The 2021 Guidance provides useful steps and questions to consider in implementing any such review.

If you have any questions or require assistance, please contact any member of the Troutman Pepper Employee Benefits and Executive Compensation Practice Group. We are here to help you in any way that we can.

---

[1] The final rules for electronic disclosures can be found here.

[2] The EBSA press release for the 2021 Guidance can be found here.

[3] For more information on the report, see ERISA Advisory Council Report, Cybersecurity Considerations for Employee Benefits Plans (November 2016).

[4] *Bartnett v. Abbott Labs., et al*., No. 20-CV-02127, 2021 WL 428820 (N.D. Ill. Oct. 10, 2020) and *Bartnett v.*

Abbott Labs., et al., No. 20-CV-02127, 2021 WL 428820 (N.D. Ill. Feb. 8, 2021).

RELATED INDUSTRIES + PRACTICES

- Employee Benefits + Executive Compensation