RETIREMENT PERSPECTIVES

Protecting Your Retirement Plan from Cybersecurity Threats

July 28, 2021

Brian Dobbis, QKA, QPA, QPFC, TGPC
Director, Retirement Solutions

ERISA-covered retirement plans have entered the digital world. Recent DOL guidance has made it clear that cybersecurity is part of a plan sponsor's fiduciary obligation under ERISA.

Read time: 4 minutes

With an estimated 34 million defined benefit plan participants and 106 million defined contribution plan participants covering assets of $9.3 trillion, it's clear the stakes are high when it comes to protecting the retirement system from cyber criminals.[1] Think about it: ERISA-covered retirement plans maintain a treasure trove of personal data on participants (e.g., social security number, address, etc.). That makes these plans an extremely tempting target for criminals. Without sufficient protection, participants' personal data and assets are at risk from cybersecurity threats.

"The recordkeeping industry has built and operates vigorous systems to protect participant accounts. But no matter how vigilant your plan's recordkeeper is, plan sponsors, plan fiduciaries, and plan participants can and should take steps to protect retirement accounts from cyber theft," says Jeanne Klinefelter Wilson, Principal, Groom Law Group.[2]

First-of-Its-Kind Cybersecurity Guidance from the DOL

The Department of Labor (DOL) has made cybersecurity risk an enforcement priority and has put ERISA plan fiduciaries on notice. On April 14, 2021, the Department issued cybersecurity guidance via the Employee Benefits Security Administration (EBSA) for the first time. Prior to issuing this guidance, it was not well defined what the DOL considered to be prudent with respect to addressing cybersecurity risks.

It's generally accepted that ERISA plan fiduciaries have a degree of responsibility to reduce a plan's exposure to cybersecurity events. The DOL's new guidance goes on to state that "responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks, and the tips provided (in the guidance) are meant to "help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers."[3] Thus, an ERISA plan fiduciary needs to be vigilant when deciding whether (or not) to hire a service provider. The plan fiduciary should give consideration to the service provider's (e.g., recordkeeper, Third Party Administrator, etc.) cybersecurity controls and their documentation of such controls.

This DOL guidance is written as "tips" and "best practices" and came in three parts:

. Tips for Hiring a Service Provider: These tips help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity

Most people know you can roll over a 401(k)or a 403(b) into an IRA, but few know that a "reverse rollover" is an

practices and monitor their activities, as ERISA requires.

available option. There are pros and cons to this scenario.

2. Cybersecurity Program Best Practices: A series of 12 steps designed to assist plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks.

3. Online Security Tips: This part offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

The guidance complements EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries. These include provisions on ensuring that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems include measures calculated to protect Personally Identifiable Information (PIN).

While the guidance is based on the premise that ERISA plan fiduciaries have a duty to mitigate cybersecurity risk, the DOL also recognized that retirement plan *participants* play an important rule in safeguarding their accounts. In their "tips" sheet the DOL acknowledges that plan participants may unknowingly put their retirement savings at risk if they fail to follow safe online practices. The DOL tips advise participants to, for example, create and routinely monitor their online retirement account. Other tips include creating a strong and unique password, updating contact information, avoiding free WIFI, and reporting identity theft.

Bottom line: The DOL is ramping up enforcement, which is a sign that it takes cybersecurity seriously. What's more, plaintiffs could potentially attempt to use this new guidance as the basis for a breach of fiduciary duty.

Suggested Best Practices by DOL

Part of the guidance included a list of Cybersecurity Program Best Practices for recordkeepers and other service providers. The guidance summarizes 12 best practices that plan service providers "*should"* implement to mitigate exposure to cybersecurity risks. Although this guidance is specific to service providers, the DOL points out that plan fiduciaries should be aware of these best practices to enable them to make prudent decisions when hiring a service provider.

Plans' service providers should:

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 annual 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.

). Encrypt sensitive data, stored and in transit.

. Implement strong technical controls in accordance with best security practices.

!. Appropriately respond to any past cybersecurity incidents.

For more detail on these cybersecurity best practices, visit the DOL site **here**.

DOL Has Begun a Cybersecurity Audit Initiative

In another sign of how seriously the DOL takes this issue, it has begun a broad scale cybersecurity audit initiative. The DOL audit requests are probing and serious, and plan fiduciaries should take note. Audit requests received by some organizations have asked the plan fiduciary to produce all cybersecurity and information security program policies, procedures, and guidelines that relate to the plan, whether applied by the plan sponsor or by a vendor, as well as detailed documentation evidencing specific actions taken by the plan's fiduciaries and vendors.

This audit initiative underscores the importance for plan sponsors to review the three-part guidance issued by the DOL and begin taking actions to address it if they haven't done so already. Plan fiduciaries that fail to act promptly on this guidance take the unnecessary risk of being surprised and overwhelmed by the wide-ranging nature of the DOL's cybersecurity audit request.

Bottom line: Cybersecurity for your retirement plan is too important an issue to overlook. It's critical to ensure you have thought about how to address this risk, not just because it is on the DOL's radar, but because of the stakes for your plan and participants. Begin a series of discussions with your Service Provider, Financial Advisor, and ERISA attorney.

Key Takeaways:

- ERISA requires plan fiduciaries to take appropriate precautions to mitigate cybersecurity risks.
- The DOL has stepped up its interest and activities surrounding cybersecurity for retirement plans. It has issued a three-part guidance, a 12-step best-practice list for plan providers and has begun a cybersecurity audit initiative.
- If plan sponsors have not been paying attention to cybersecurity before now, it's time to act. If you are a plan fiduciary you should stay abreast of developments in this rapidly evolving area.
- As an ERISA fiduciary, you play a critical role in guarding retirement plan participants against the theft of their accounts by cybercriminals. Review and follow the DOL guidance while staying current of developments in this fast-developing area.

---

[1] News Release, U.S. Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, Plan Participants, April 14, 2021. Data as of 2018.

[2] Klinefelter Wilson, Jeanne, "Cybersecurity for Plan Fiduciaries: Focus on Account Theft," PLANSPONSOR, July 6, 2021

[3] Cybersecurity Program Best Practices, Employee Benefits Security Administration, Department of Labor

Investors should carefully consider the investment objectives, risks, charges and expenses of the Lord Abbett Funds. This and other important information is contained in the fund's summary prospectus and/or prospectus. To obtain a prospectus or summary prospectus on any Lord Abbett mutual fund, you can click here or contact your investment professional or Lord Abbett Distributor LLC at 888-522-2388. Read the prospectus carefully before you invest or send money.

The information provided is not directed at any investor or category of investors and is provided solely as general information about Lord Abbett's products and services and to otherwise provide general investment education. None of the information provided should be regarded as a suggestion to engage in or refrain from any investment-related course of action as neither Lord Abbett nor its affiliates are undertaking to provide impartial investment advice, act as an impartial adviser, or give advice in a fiduciary capacity. If you are an individual retirement investor, contact your financial advisor or other fiduciary about whether any given investment idea, strategy, product or service may be appropriate for your circumstances.