DOL's Cybersecurity Guidance: Practical Pointers for Fiduciaries

May 17, 2021 – CLIENT ALERT

On April 14, 2021, the Department of Labor ("DOL") issued important guidance concerning cybersecurity in relation to ERISA-covered employee benefit plans, with separate items directed chiefly to service providers, fiduciaries, and participants and beneficiaries (referred to in this Client Alert as "participants"). This guidance comes in the wake of several lawsuits involving the hijacking of and theft from participants' DC plan accounts, considerable media coverage of the issue, and, most immediately, a February 11, 2021, U.S. Government Accountability Office ("GAO") report on the issue (the "GAO Report"). (See "DEFINED CONTRIBUTION PLANS, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (GAO-21-25), available at https://www.gao.gov/assets/gao-21-25.pdf.)

This Client Alert will review the GAO Report for context and background, and then discuss the DOL's first foray into guidance concerning cybersecurity in the context of ERISA-covered employee benefit plans.

Background and Context

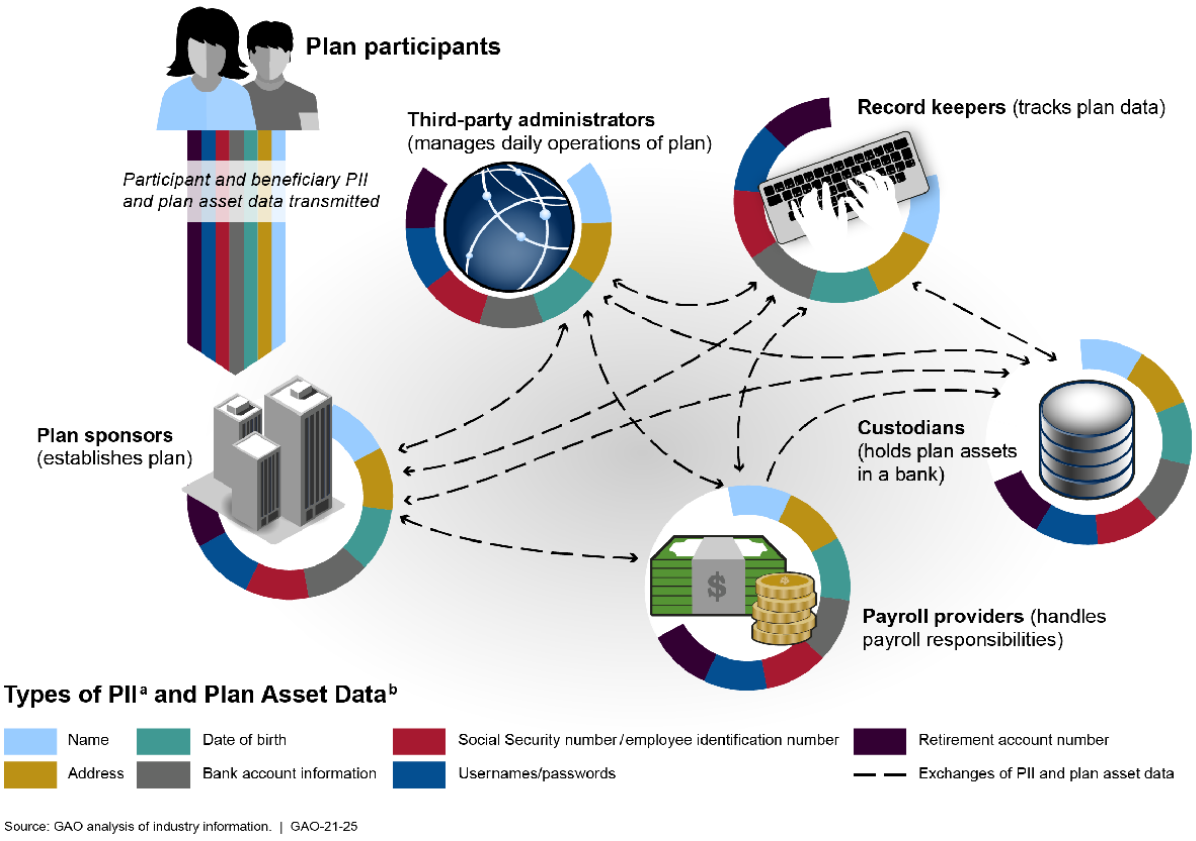
The GAO Report notes that "DC plans have in recent decades become the dominant employer-sponsored retirement plan type in the private sector," and that as of 2018, 106 million people participated in private sector DC plans, which held assets of nearly $6.3 trillion.

The GAO Report also notes that there "is no comprehensive federal guarantee of 401(k) plan benefits lost, for example, due to poor investment decisions by the employee or other reasons, such as theft." It further reports that "a vast amount of PII and plan asset data" is shared by and among DC plan sponsors and service providers in the ordinary course of administering a DC plan, and usefully provides the following definitions:

- **"PII" or "personally identifiable information"** is "any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number; and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information."

- **"Plan asset data"** is "sensitive information that is associated with a participant's retirement assets, such as their retirement account number and bank account information."

The data flow for this information is illustrated in the GAO Report (at p. 13) as follows:



As illustrated, there are many data transfers and storage locations, each of which is potentially at risk. The GAO report characterizes this as "a vast amount of PII and plan asset data" that is subject to "substantial sharing." The nature and importance of this data, combined with the extent of its collection and sharing, led the GAO Report to characterize this as creating "significant" cybersecurity risks for DC plans.

The GAO Report notes that some actors ("threat actors") seek to steal only participant PII, while others seek to steal the assets held in DC plan accounts through an "account takeover." As explained in the GAO Report:

> *Account takeover occurs when a threat actor fraudulently transfers assets out of an account, such as a retirement plan account. After gaining access to the account, the threat actor collects information that can be used repeatedly to initiate fraudulent transactions. For example, a threat actor might gain access to a retirement account online and divert funds to their own bank account.*

This Client Alert refers to an account takeover as a "hijacking."

The GAO Report next describes Federal rules designed to mitigate cybersecurity risk, namely the Gramm-Leach Bliley Act ("GLBA") and the Federal Trade Commission Safeguards Rules (which implement the security requirements of the GLBA), but notes that these may not apply to all of the parties who receive, transfer, and hold PII and plan asset data. Further, as the GAO Report points out, other guidance and tools offered by the Federal government, such as by the National Institute of Standards and Technology and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, are generally voluntary and thus cannot ensure that parties are, in fact, taking appropriate steps to mitigate cybersecurity risk.

The GAO Report recognizes various financial and retirement industry efforts to develop information sharing efforts and leading practices and standards designed to assist companies with mitigating cybersecurity risks, including those by the Society of Professional Asset Managers and Record Keepers Institute (the "SPARK Institute," which has various cybersecurity and fraud resources available on its website), the AICPA (which developed the "SOC 1" and "SOC 2" cybersecurity risk management assessments), the Financial Services Information Sharing and Analysis Center (FS-ISAC), and providers of cybersecurity insurance.

> **PRACTICE POINTER:** It is important to determine whether cybersecurity insurance would cover losses incurred by a participant whose DC plan account was hijacked and stolen; if so, the conditions for coverage (for example, only if the participant was diligent in protecting their PII and log-in credentials against disclosure); and how it is to be determined whether the conditions have been met.

Finally, the GAO Report reviewed DOL activity and ultimately summarized its recommendations and DOL's response as follows:

> *GAO is making two recommendations to DOL to formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in DC plans and to establish minimum expectations for addressing cybersecurity risks in DC plans. DOL agreed with GAO's second recommendation but did not state whether it agreed or disagreed with the first one. GAO believes both recommendations are warranted.*

DOL Guidance

Before getting to the specifics of the DOL guidance, we note that the DOL responded clearly to the GAO's first recommendation, stating that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks." It is helpful that the DOL refers (as did GAO) only to "mitigation" of cybersecurity risks, recognizing that it may not be possible to fully eliminate these risks at all times. This also reflects ERISA's duty of prudence, which looks to all of the facts and circumstances of a situation. Further, while a well-advised fiduciary might already consider cybersecurity of DC plan PII and plan asset data within the purview of their fiduciary duties, this is a welcome and clear affirmation of this principle.

As to the specifics, there are three DOL pieces of sub-regulatory guidance, which to some extent interlock with one another:

- Cybersecurity Program Best Practices – This is "for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire," and may be useful as well to participants in evaluating the extent to which service providers and fiduciaries have met their obligations.

- Tips for Hiring a Service Provider with Strong Cybersecurity Practices – This is designed "[t]o help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor . . . service providers," and may be useful as well to service providers, as well as to participants in evaluating the extent to which service providers and plan fiduciaries have met their obligations.

- Online Security Tips – This is directed at participants, and may be useful as well to plan fiduciaries and service providers.

Cybersecurity Program Best Practices

As noted above, these "best practices" are not only for use by service providers, but also "for plan fiduciaries making prudent decisions on the service providers they should hire." The clear message here is that a prudent fiduciary should ask about and consider whether and to what extent a potential service provider follows these best practices.

As to specific best practices relating to protection of participant PII and plan asset data, the DOL states that 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 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. Appropriately respond to any past cybersecurity incidents."

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

The DOL's tips include the following:

- "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."
- Review "public information regarding the service provider's information security incidents, other litigation, and legal proceedings relating 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 that would cover losses caused by cybersecurity and identity theft breaches," both internal (by employees) and external (for example, threat actor hijacking and stealing from a participant account).
- "When you contract with a service provider, make sure that the contract 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." Also, "[t]ry to include terms in the contract that would enhance cybersecurity protection for the [p]lan and its participants" (for example, regarding information security reporting, the use and sharing of information and confidentiality, notification of security breaches, and compliance with records retention and destruction, privacy and information security laws).

> **PRACTICE POINTER:** Over the last several years, DC plan recordkeepers have starting offering "participant guarantees," that is, promises to make a participant whole for losses resulting from account hijacking (provided the participant has exercised reasonable care in protecting their PII). Fiduciaries should ask potential and incumbent DC plan recordkeepers if they provide a participant guarantee. If so, fiduciaries and their legal counsel should review the applicable documentation to determine, among other things, what situations are covered, what may be required of the plan sponsor and participants, and how incidents will be investigated, and should consider whether and, if so, how the guarantee may be incorporated into the service agreement.

Online Security Tips

These tips, which as noted above are directed at plan participants, are practical suggestions that should be encouraged. They send a message that participants play a critical role in and have a responsibility for safeguarding their own PII and plan asset data, and therefore should exercise diligence. The tips – each of which is supplemented by more detailed explanation and comments by the DOL – are as follows:

- Register, set up and routinely monitor your 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

Additional Observations and Practice Pointers

Cybersecurity Best Practices and Tips for Hiring a Service Provider with Strong Cybersecurity Practices

The Cybersecurity Best Practices can be useful, together with the Tips for Hiring a Service Provider, for plan fiduciaries in selecting, contracting with, and monitoring service providers. For example:

- When searching for a service provider, incorporate the Cybersecurity Best Practices into the requirements of the Request for Proposal, and evaluate the responses accordingly.

  > **PRACTICE POINTER:** Fiduciaries should consider whether they or their consultant have sufficient expertise to evaluate service provider responses to cybersecurity questions; if they do not, they should obtain expert review and advice, whether from other in-house resources or from an outside consultant.

- Service provider agreements should address all parties' obligations concerning cybersecurity measures.

  > **PRACTICE POINTER:** For legitimate reasons, service providers may not want to share details of their cybersecurity programs. Nonetheless, the agreement should include a reasonable degree of specificity, which the DOL's best practices may provide.

- The Cybersecurity Best Practices can serve as at least a partial list of cybersecurity topics for fiduciaries to consider as they monitor service provider performance (e.g., by ensuring that the service provider conducts an annual risk assessment, conducts appropriate training, and exercises due diligence regarding cloud-based systems and services).

Both the Cybersecurity Best Practices and the Tips for Hiring a Service Provider with Strong Cybersecurity Practices will likely be used by the DOL and participants as standards against which service provider and fiduciary conduct concerning cybersecurity will be measured.

> **PRACTICE POINTER:** As with all aspects of fiduciary decision making and monitoring, fiduciaries should be sure to document their collection, review, and assessment of cybersecurity program information from potential and incumbent service providers.

Although the GAO Report focused on DC plans, the DOL guidance is not limited to DC plans; in particular, the DOL's Tips for Hiring a Service Provider with Strong Cybersecurity Practices specifically refers to 401(k) plans "and other types of pension plans." Thus, fiduciaries of defined benefit plans should consider these issues and this guidance as well. Further, many of the concepts and guidelines may also be useful in relation to health and welfare plans.

Conceptually, the guidance is just an extension into the cybersecurity context of what well-advised fiduciaries already know about prudent service provider selection and oversight. And although cybersecurity is certainly important, it should not be the only, or necessarily the most important, criterion to consider in making selection decisions. Rather, cybersecurity should be considered as one of many relevant criteria, such as experience, quality, participant experience, and price.

Online Security Tips

These are obviously directed at participants. However, they may be useful to plan fiduciaries in carrying out their fiduciary duties in helping to protect participant PII, plan asset data, and plan account balances. Also, to the extent a recordkeeper provides make-whole relief to participants for losses resulting from account hijacking, these tips may be used as a standard for determining whether the participant took appropriate steps to protect their account.

> **PRACTICE POINTER:** Fiduciaries may want to post copies of the Online Security Tips on HR or benefit portals, or on the plan's website. They may also want to distribute copies to participants along with other mailings as appropriate.

Conclusion

The DOL's cybersecurity guidance is a useful and practical foray into the complex and constantly changing cybersecurity landscape. The informal and specific nature of the guidance should foster review and use by service providers, plan fiduciaries, and participants,

and thus lead to better cybersecurity efforts and concrete steps to protect participant savings – certainly a welcome development.

Please contact us if you have questions. We are happy to help evaluate issues and collaborate on projects to review your policies and procedures to help ensure they are reasonable under the circumstances and consistently implemented by service providers.

Keightley & Ashner LLP
One Metro Center, 700 12th Street, N.W., Suite 700, Washington, D.C. 20005
Phone: (202) 558-5150
Fax: (202) 330-5490
Email: info@keightleyashner.com
Website: https://keightleyashner.com