Volume 94 – September 2021

INTERNATIONAL PENSION LAWYER

Journal of the International Pension and Employee Benefits Lawyers Association

INTERNATIONAL
PENSION LAWYER

Contents

September 2021 – No 94

INTERNATIONAL
PENSION LAWYER

DOL's Cybersecurity Guidance: Practical Pointers for Fiduciaries

Elliot Raff

Keightley & Ashner LLP

elliotraff@keightleyashner.com

United States

Introduction

Over the last 10 years, the Advisory Council on Employee Welfare and Pension Benefit Plans (known as the "ERISA Advisory Council")[1] raised concerns and warnings about cybersecurity threats to private sector employee benefit plans. More recently, over the last few years, litigation has emerged arising from "account takeovers" of and thefts from individuals' private retirement accounts, and the United States General Accounting Office ("GAO") conducted a formal study of cybersecurity issues as they relate to defined contribution retirement plans ("DC Plans"). Following the GAO's report, the United States Department of Labor ("DOL") issued significant informal guidance on these issues.

This article will provide an overview of legal and practical considerations in the United States relating to cybersecurity issues for DC Plans.

1. United States DC Plan environment

The best source for understanding cybersecurity issues in the US DC Plan environment is the February 11, 2021, GAO report referenced above, "Defined Contribution Plans, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (GAO-21-25) (the "GAO Report").[2]

The GAO Report notes that "DC plans have in recent decades become the dominant employer-sponsored retirement plan type in the private sector" of the United States, 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 [DC 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

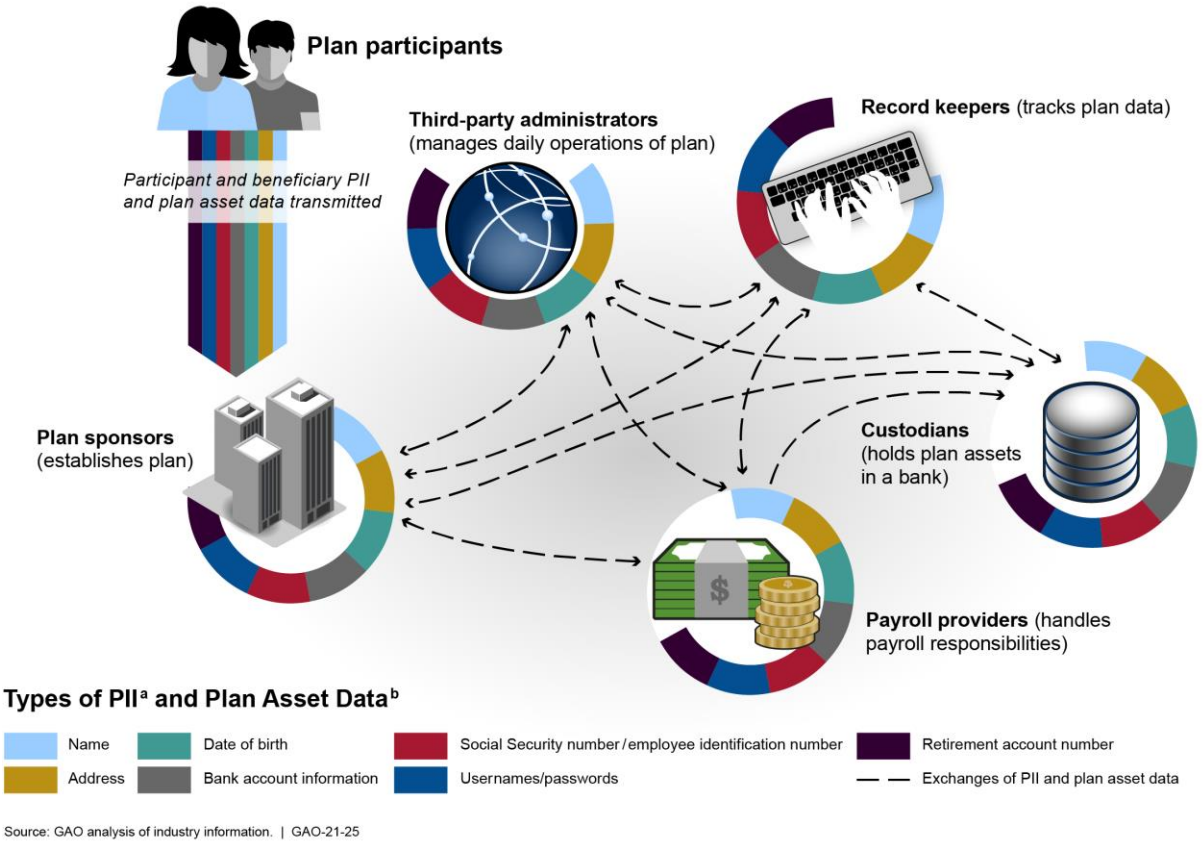
[1] The ERISA Advisory Council's duties are to advise the Secretary of Labor and make recommendations regarding the Secretary's functions under the United States Employee Retirement Income Security Act ("ERISA"). It is made up of 15 members representing employee organizations (labor unions), employers, the general public, and the fields of insurance, corporate trust, actuarial counseling, investment counseling, investment management, and accounting.

[2] The GAO Report is available at <https://www.gao.gov/assets/gao-21-25.pdf>.

Plan sponsors (*i.e.*, employers) and service providers in the ordinary course of administering a DC plan, and provides the following definitions:[3]

- "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. Further, new data is constantly being added to these data routes, for example, after each payroll period, the Payroll provider or Plan Sponsor provides a payroll report with participant compensation and contributions to the recordkeeper. The GAO Report characterizes this as "a vast amount of PII

[3] Although the definition of PII is similar to definitions under the laws of various specific States, the presence of this definition in the GAO Report does not make it a legally sanctioned or required definition.

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.

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 ("NIST") and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA"), 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 Association of International Certified Professional Accountants ("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.

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.

2. Legal issues

The key legal issues relate to obligations to protect PII and plan asset data in transit and at rest. Some entities involved in DC Plan operations, such as bank custodians, are subject to cybersecurity obligations under applicable banking law. Other entities, such as Record Keepers and Third-Party Administrators, are not subject to these — or any other — State or Federal regulatory standards. And, as indicated above, while there are standards

established by United States government agencies, such as NIST and CISA, and private associations, such as the SPARK Institute, those standards are voluntary. Consequently, it is possible that a DC Plan Record Keeper and/or Third-Party Administrator may not adhere to any legally required or voluntary cybersecurity standards (although many, if not most, do).

Further, the United States Employee Retirement Income Security Act ("ERISA") imposes liability on persons who stand in a fiduciary relationship to DC Plans, a relationship characterized by the person formally being delegated (either by the Plan document or appropriate corporate action) or, under the circumstances, having de facto discretion over a DC Plan's administration, operations, and/or disposition of assets. With the exception of Custodians, typically, DC Plan service providers do not take on or in fact have such discretion; true, a Record Keeper may process requests for distributions and apply investment instructions, but they do so by following detailed procedures designed to eliminate discretion and make the function "merely ministerial" and thereby avoid fiduciary status. Service providers not being fiduciaries is the basis upon which nearly all DC Plan service provider contracts are drafted. As a result, except in unusual situations (where service providers significantly deviate from their internal procedures), these DC Plan service providers are not treated as fiduciaries and their conduct is not subject to ERISA's fiduciary standards of care. This, combined with the absence of State law establishing standards, may leave claimants without effective legal recourse.

These same circumstances create legal uncertainties and challenges for those who are fiduciaries of DC Plans, typically a committee of executive-level employees of the Plan Sponsor. In the current DC Plan environment, with most functions outsourced, the primary fiduciary duties are to prudently select and then monitor service provider services and functions. Nonetheless, fiduciaries are ultimately accountable and can be held liable for DC Plan operations. As such, whether cybersecurity of DC Plan data is a fiduciary obligation — and, if so, the scope of such obligations — has been of great concern to fiduciaries. Until the recent DOL guidance, however, the DOL had not made any clear pronouncements on this question, and so there was some uncertainty relating to the role of fiduciaries in grappling with cybersecurity in relation to their DC Plans.

These issues are illustrated by emerging DC Plan account takeover litigation. With varying degrees of specificity, these complaints ultimately allege that someone other than the Plan Participant accessed the Participant's DC Plan account, and was able to effect a withdrawal of funds. For example, in *Bartnett v. Abbott Laboratories, et al.*, No. 1:20-cv-02127 (N.D. Ill 2020), Ms. Bartnett alleged that someone (the "cyberthief") entered her email on the Record Keeper's DC Plan Participant web portal, clicked "Forgot Password," opted to reset the password via email, intercepted the email, and changed the password, thereby capturing her log-in credentials. Thereafter, she alleged, the cyberthief changed her banking information, and then requested and obtained withdrawals totaling approximately $245,000. Ms. Bartnett further alleges various claimed procedural failures by the Record Keeper, such as sending transaction confirmations by physical mail rather than email and missing "red flags" during telephone interactions with the cyberthief.

Ms. Bartnett brought claims against Abbott Laboratories, her former employer, the Abbott Laboratories executive who served as the plan fiduciary, and against the Record Keeper, alleging violations of ERISA's fiduciary duties and, as to the Record Keeper, various State law claims. Initially, the Court dismissed Abbott Laboratories and the individual who served as plan fiduciary based on, among other things, its conclusion that ERISA's fiduciary duties do not extend to "safeguarding of data and prevention of scams." The Court did, however, conclude that the Record Keeper could be treated as a fiduciary based on its control over the DC Plan's assets (processing the distributions) and Ms. Bartnett's allegations disputing the Record Keeper's assertion that its actions were purely ministerial. Ms. Bartnett filed an amended complaint alleging that Abbott Laboratories and the plan fiduciaries failed to act prudently in selecting and monitoring the Record Keeper, with extensive allegations about prior alleged data breaches. Ultimately, the case settled and these claims were dismissed.

The Record Keeper in *Bartnett* is highly reputable, one of the largest DC Plan Record Keepers in the United States, and invests tremendous sums in its cybersecurity infrastructure. Nonetheless, the *Bartnett* case illustrates the relative ease with which cyberthieves can beat systems with relatively little PII (name, email). And, while Ms. Bartnett was able to convince the Court that the Record Keeper could be treated as an ERISA fiduciary, that conclusion was based on the very specific circumstances in the case — facts that, assumed to be true, could reasonably be viewed as crossing the line from ministerial to discretionary conduct.

In the context of this litigious environment, the DOL issued three items of informal guidance relating to cybersecurity, ERISA, and DC Plans.

3. 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[1]– This is "for use by Record Keepers 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".
- Tips for Hiring a Service Provider with Strong Cybersecurity Practices[2] – This is designed "[t]o help business owners

1 <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf>.

2 <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for- hiring-a-service-provider-with-strong-security-practices.pdf>.

and fiduciaries meet their responsibilities under ERISA to prudently select and monitor … service providers".

- Online Security Tips[3] – This is directed at Participants.

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 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."

[3] <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf>.

- "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).

It is worth noting that, over the last several years, DC Plan Record Keepers 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 Record Keepers if they provide a Participant guarantee. If so, fiduciaries and their legal counsel should review the applicable documentation to determine, among other things, what law applies (typically the law of the State where the Record Keeper is located), 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.

- "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).

It is worth noting that, over the last several years, DC Plan Record Keepers 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 Record Keepers if they provide a Participant guarantee. If so, fiduciaries and their legal counsel should review the applicable documentation to determine, among other things, what law applies (typically the law of the State where the Record Keeper is located), 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.

4. Additional observations

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.
    - 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.
    - 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.
    - 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 Record Keeper 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.
- 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.

Elliot Raff is Senior Counsel Compensation & Benefits at US law firm Keightley & Asher LLP.