TRUCKER ✦ HUSS

BENEFITS REPORT

SPECIALIZED TALENT & EXPERTISE TO SOLVE THE MOST COMPLEX OR STRAIGHTFORWARD CLIENT CHALLENGES.

With more than 25 attorneys practicing solely in employee benefits law, Trucker Huss is one of the largest employee benefits specialty law firms in the country. Our in-depth knowledge and breadth of experience on all issues confronting employee benefit plans, and their sponsors, fiduciaries and service providers, translate into real-world, practical solutions for our clients.

A DIVERSE CLIENT BASE. We represent some of the country's largest companies and union sponsored and Taft-Hartley trust funds. We also represent mid-sized and smaller employers, benefits consultants and other service providers, including law firms, accountants and insurance brokers.

PERSONAL ATTENTION AND SERVICE, AND A COLLABORATIVE APPROACH. Since its founding in 1980, Trucker Huss has built its reputation on providing accurate, responsive and personal service. The Firm has grown in part through referrals from our many satisfied clients, including other law firms with which we often partner on a strategic basis to solve client challenges.

NATIONALLY-RECOGNIZED. Our attorneys serve as officers and governing board members to the country's premier employee benefits industry associations, and routinely write for their publications and speak at their conferences.

TRUCKER ✦ HUSS

A PROFESSIONAL CORPORATION

ERISA AND EMPLOYEE BENEFITS ATTORNEYS

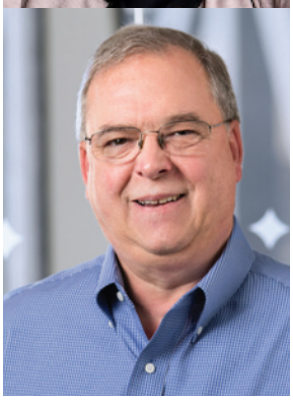
One Embarcadero Center, 12th Floor
San Francisco, California 94111-3617

15821 Ventura Blvd, Suite 510
Los Angeles, California 91436-2964

Tel: (415) 788-3111
Fax: (415) 421-2017
Email: info@truckerhuss.com

www.truckerhuss.com

Participant Data: Plan Asset or Fair Game for Recordkeepers to Use to Market Non-Plan Products?



CATHERINE REAGAN AND R. BRADFORD HUSS

APRIL 2021

In an emerging theory of liability, plan fiduciaries' treatment of participants' personal data is coming under scrutiny. Over the last five years, we have seen how the collection of many individuals' personal data can become a valuable asset in the right hands — whether it's used to influence an election, design a marketing plan that targets individuals based on their specific preferences and needs, or just to compile large troves of information to analyze trends. *See "The World's Most Valuable Resource Is No Longer Oil, But Data,"* The Economist (May 6, 2017). Participants' awareness of, and concerns regarding, the collection, use, sale, and transfer of personal data is evolving. In today's world, where data is considered as valuable as other commodities, it is not surprising that the way plan fiduciaries look at protecting participants' personal data is changing. What is surprising is that Employee Retirement

INDIVIDUAL ARTICLES WILL BE AVAILABLE AT TRUCKERHUSS.COM/PUBLICATIONS

IN THIS ISSUE...

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

Income Security Act of 1974 (ERISA) litigation is one new avenue being used to try to force plan fiduciaries to protect participants' data.

As part of a broader wave of "excessive fee" lawsuits involving 401(k) and 403(b) plans, three lawsuits were filed against prominent universities involving, among other aspects, claims concerning the use of participant data: New York University ("NYU 2")[1]; Northwestern University[2]; and Vanderbilt University. In another three 403(b) excessive fee cases — against John Hopkins University, MIT, and Emory University — participant data cross-selling restrictions were included in the settlements, even though claims regarding cross-selling were not raised in the complaints.[3] At first, participant data claims seemed limited to 403(b) plans, but in 2020, that litigation expanded to include two 401(k) plans sponsored by ADP TotalSource Group[4] and Shell Oil Company. These are referred to below collectively as the "Participant Data Cases."

In the Participant Data Cases, participant plaintiffs allege that third-party administrators and recordkeepers are using participants' personal data to cross-sell profitable non-plan products to plan participants. Such personal data includes:

- Identifying Information: i.e., participant's name, contact information, social security number, date of birth, marital status, phone numbers, and work and personal email addresses;
- Financial Information: i.e., income levels, contribution history, account balance, and expected retirement age; and
- Investment Preferences: i.e., investment histories and investment holdings.

The plaintiffs allege that recordkeepers are soliciting participants to purchase expensive and lower rate of return non-plan products such as Individual Retirement Accounts (IRAs) and Individual Retirement Annuities, high-interest credit cards, life insurance, banking products, advisory accounts, individual brokerage accounts, and options trading accounts.

The plaintiffs in these Participant Data Cases allege that plan fiduciaries (1) breached their fiduciary duty and (2) allowed prohibited transactions to occur when they did not prevent recordkeepers from using participants' personal data to cross-sell non-plan products. Under ERISA's strict fiduciary standards, selecting and monitoring plan service providers, such as recordkeepers for a plan, is a fiduciary function. Fiduciaries must act for the exclusive purpose of providing benefits to participants and their beneficiaries, and defraying the reasonable expenses of administering the plan. In an action against plan fiduciaries alleging a breach of fiduciary duty concerning plan assets, fiduciaries can be personally liable, and any recovery may be for the benefit of the entire plan.

Participant Data Case plaintiffs are seeking restitution on behalf of their plans for allegedly unjust profits that recordkeepers earned using participant data; or alternatively, they seek a surcharge against the fiduciaries for the value of the participant data that recordkeepers used. Although plaintiffs are seeking relief on behalf of the plan generally, these are defined contribution plans — so any recovery would likely be allocated into each participant's individual account. The plaintiffs are also seeking injunctive relief to prevent future use of participant data for cross-selling purposes.

This article addresses: the general participant data claims that have been raised in defined contribution plan excessive fee complaints; the Seventh Circuit's decision in *Divane v. Northwestern University*; the more sophisticated arguments being raised after *Northwestern University*, particularly in the *Shell Oil Company* case; and the trend in some Participant Data Case settlements to include cross-selling restrictions.

I. Participant Data Claims Generally

In the Participant Data Cases, the plaintiffs consistently allege that participant data is a plan asset and that defendants allowed recordkeepers to use highly confidential personal information of participants and retirees to sell the recordkeepers' investment and wealth management products. The plaintiffs argue that defendants breached their fiduciary duty and caused the plan to engage in prohibited transactions with the recordkeepers by (1) enabling recordkeepers to profit from their role as plan service providers (outside of the fees negotiated in the service agreements) and (2) failing to protect valuable plan assets (the participants' data). To support the second argument,

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

participants hinge their case on one core underlying premise: that participant data is a plan asset that plan fiduciaries have an obligation to protect under ERISA.

Participant data claims first arose in 2017, after a non-ERISA whistleblower complaint filed with the SEC raised concerns about recordkeepers' use of participant data in ERISA plans. The whistleblower alleged that a recordkeeper for many 403(b) plans, TIAA-CREF, used participants' data to engage in allegedly abusive practices to solicit participants' purchase of its own more expensive non-plan products. According to the whistleblower, recordkeeper-affiliated financial planners would use scare tactics during educational opportunities to try to sell more expensive non-plan products to participants of TIAA-CREF's existing retirement plan clients. In response to the whistleblower complaint, in 2019, TIAA-CREF did an internal review, updated all of their training materials and settled with the SEC regarding the allegations. Without acknowledging fault, TIAA-CREF agreed to (1) correct necessary disclosures, (2) evaluate whether clients should be moved to lower-cost share classes, and (3) review their policies and procedures regarding disclosures for their mutual fund class selection. In the Participant Data Cases filed under ERISA, we have seen plaintiffs cite to articles referencing this whistleblower complaint, and the alleged predatory practices, to support their participant data claims.

So far, no courts have accepted the legal theory that participant data is a plan asset under ERISA — however, several pending cases may determine the ultimate outcome of this new theory of liability.

II. *Divane v. Northwestern University*

In *Divane v. Northwestern University*, 2018 WL 2388118 (N.D. Ill. May 25, 2018), aff'd, 953 F.3d 980 (7th Cir. 2020), *petition for cert. filed*, (U.S. Jun. 19, 2020) (No. 18-2569), the district court became the first court to rule on the participant data theory of liability. The district court dismissed the plaintiffs' first amended complaint and denied their request for leave to file a second amended complaint which included new participant data allegations. The parties briefed the issue, and the district court found that the plan fiduciaries did not breach their fiduciary duty by allowing recordkeepers to have access to participants' confidential information, which is required to perform necessary recordkeeping functions. The district court noted that the plaintiffs failed to "cite[] a single case in which a court has held that releasing confidential information or allowing someone to use confidential information constitutes a breach of fiduciary duty under ERISA." *Northwestern Univ.*, 2018 WL 2388118, at *12. Nor do plaintiffs provide any support that participant data is a plan asset in a prohibited transaction. While participant data does have some value, it is not a plan asset under "ordinary notions of property rights." *Id.* Finding the plaintiffs' arguments with respect to participant data posed too abstract an injury for standing purposes, the district court denied the request for leave to file the proposed second amended complaint.

The Seventh Circuit affirmed the district court's order dismissing the action. Without specifically addressing the participant data claims, the Seventh Circuit determined leave to amend was futile as all the new claims in the second amended complaint — including the participant data claims — were essentially the same claims in different counts, and therefore improperly pled. The plaintiffs filed a petition for certiorari to the U.S. Supreme Court challenging the dismissal of the first amended complaint and the decision to deny leave to amend, which is pending.[5]

III. *Harmon v. Shell Oil Company*

A year to the month after the Seventh Circuit decided the *Northwestern University* 403(b) plan case, participant data allegations were front and center in a 401(k) plan excessive fee case, *Harmon v. Shell Oil Company, et al.*, No. 3:20-cv-00021, 2021 WL 1232694 (S.D. Tx. Mar. 30, 2021), where another district court rejected the legal theory that participant data is a plan asset. In *Shell Oil Company*, unlike the other Participant Data Cases, the plaintiffs included allegations against the plan recordkeeper, Fidelity, as a co-defendant. All allegations against the recordkeeper were premised on the legal theory that participant data is a plan asset. Ordinarily, recordkeepers do not exercise discretion over plan assets and are not plan fiduciaries. In *Shell Oil Company*, the plaintiffs alleged that the recordkeeper was a plan fiduciary because it had control over the participants' data, which was alleged to be a plan asset. When the recordkeeper brought a motion to dismiss, the entire focus was on the participant data claims. With the issue of whether participant data is a plan asset now determinative of the outcome for the recordkeeper, it raised novel arguments against this

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

legal theory that had not been addressed in the prior Participant Data Cases.

First, the recordkeeper argued that the plaintiffs failed to establish Constitutional standing under Article III because they lacked an injury in fact. The recordkeeper asserted that the plaintiffs failed to allege that plan participants actually transferred assets out of the plan to their detriment on the basis of the recordkeeper's cross-selling solicitations, as opposed to other reasons. The recordkeeper also argued that simply soliciting participants a few times was insufficient to establish an injury. The plaintiffs countered that at least one named plaintiff rolled money out of the plan based on the recordkeeper's solicitation and was injured because the IRA into which he rolled money charged higher administration costs than the amounts charged to his account in the plan. The recordkeeper responded to that argument by pointing out that the amended complaint is devoid of actual comparisons showing that the named plaintiff's plan funds were rolled into more expensive IRA funds than the plan's investments.

Second, the recordkeeper asserted that ERISA's statutory framework requires that plan assets be held in trust for the exclusive benefit of plan participants and beneficiaries, which it argues is not practical when applied to phone numbers, e-mail addresses, and investment history. Plan participants have access to and may disseminate this information outside of the plan, including when they go to a competitor for financial products. The recordkeeper also releases this information in the aggregate to data collection agencies that collect information to help advise plan fiduciaries.

The plaintiffs countered that it is the compilation of each participant's data into a comprehensive financial picture, including the participant's personal data, call notes, information on major life events, investment history, and goal retirement dates, that they are referring to as a plan asset. In this way, the plaintiffs argued, participants can still use their personal information, and it does not affect the fiduciaries' exclusive control of a plan asset (the compilation of each participant's data that is held only by the recordkeepers).

Third, the recordkeeper argued that the plaintiffs' theory of participant data as a plan asset is unworkable under ERISA. There are two regulations defining plan assets under ERISA, 29 C.F.R. Section 2510.3-101 (defining plan assets in the context of plan investments) and 29 C.F.R. Section 2510.3–102 (defining plan assets in the context of participant contributions). No regulatory body has ever found that participant data is a plan asset. Also, the DOL allows plans to file a Form 5500-SF if the plans' assets can be readily valued. The recordkeeper argued that if participant data is a plan asset, it would be difficult for any plans to place a value on such an asset and, as a result, no plan would be able to file a Form 5500-SF, making this form superfluous. Further, a finding that participant data is a plan asset would affect all plans, not just ERISA defined contribution plans. The recordkeeper went on to argue that if the case progresses past the motion to dismiss phase, it will have to use participant data in its defense — which would be a breach of fiduciary duty in and of itself if participant data is a plan asset.

Finally, the recordkeeper argued that the weight of legal precedent shows that participant data cannot be a plan asset, relying on *Northwestern University* (7th Cir. 2020) (discussed above), and two other ERISA cases decided in another context: *Patient Advocates, LLC v. Prysunka*, 316 F. Supp. 2d 46 (D. Me. 2004) (an ERISA preemption case involving a state statute requiring disclosure of health plan participants' data), and *Walsh v. Principal Life Insurance*, 266 F.R.D. 232 (S.D. Iowa 2010) (finding recordkeepers could access and use participant data to send letters soliciting retail products, but the case did not address whether participant data is a plan asset).

The plaintiffs countered these arguments by asserting that they were inconsistent with the recordkeeper's position in other litigation against former employees of the recordkeeper and in internal memos of the recordkeeper that referred to customer information as being the recordkeeper's proprietary information that was as valuable as "the formula of Coke to Coca-Cola." Armed with the recordkeeper's analogy of the value of participant data, the plaintiffs attempted to rebut the legal precedent cited by the recordkeeper by referencing decades of SEC and insurance brokerage cases that treat customer data as an asset. The plaintiffs alleged the recordkeeper went to great lengths in internal memos, policies, and litigation to prevent competitors from using participants' data collected by the recordkeeper to sell competing products. The

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

plaintiffs further alleged that recordkeepers who cross-sell non-plan products consider participants' data as their own proprietary information, even though they only have access to this information by virtue of their position as a recordkeeper to the plan.

The district court in *Shell Oil Company* found that participant data is not a plan asset. In a succinct and well-reasoned opinion, the court focused on two main questions: (1) Have any other courts found that participant data is a plan asset? and (2) Is participant data an asset ERISA was designed to protect? In oral arguments, the plaintiffs conceded that no courts have found participant data to be a plan asset. The *Shell Oil Company* district court, like the district court in *Northwestern University*, declined to be the first court to make such a finding — noting the three prior ERISA cases that expressly contradict plaintiffs' arguments that participant data is a plan asset.[4] As to the second question, the *Shell Company* court focused on ERISA's statutory language which states "plan assets [are] defined by such regulations as the Secretary [of Labor] may prescribe." (citing 29 U.S.C. § 1002(42)). The court noted that there are no regulations that describe participant data as a plan asset, and the only two regulations that define plan assets do so in the context of investments and contributions. Finding that participant data is not a plan asset, the court held that the recordkeeper was not a fiduciary and had not engaged in prohibited transactions by using participant data for profit, and dismissed all claims against the recordkeeper. The next day, the district court also dismissed the participant data claims against Shell Oil Company and the plan's trustees for the same reasons.

IV. Settlement Agreements Restricting Recordkeepers' Use of Participant Data

While the issue of using participant data to cross-sell non-plan products is still developing in the courts, settlements in four of the 403(b) excessive fee cases, Emory, John Hopkins, MIT, and Vanderbilt, included provisions limiting recordkeepers' use of participant data for cross-selling purposes. In all four settlements, the recordkeeper is permitted to use participant data in situations where the participant initiates a conversation about the recordkeeper's other products.

For example, in the case involving Emory University's 403(b) plan, the settlement requires that Emory University prohibit recordkeepers from:

> Us[ing] information received as a result of providing services to the Plans and/or the Plans' participants to solicit the Plans' current participants for the purpose of cross-selling non-Plan products and services, including, but not limited to, Individual Retirement Accounts ('IRAs'), non-Plan managed account services, life or disability insurance, investment products, and wealth management services, unless in response to a request by a Plan participant.

Similar restrictions are mirrored in the other settlements referencing participant data. These settlement agreements are limited to the individual cases that settled and don't necessarily lend support for plaintiffs' participant data allegations generally; however, it is advisable for plan fiduciaries to be aware of provisions that protect participant data in other plans' recordkeeping agreements so that they can decide whether to include such provisions in their own recordkeeping contracts.

Conclusion

It remains to be seen how the courts may further rule on the issue of whether participant data is a plan asset under ERISA. So far, one district court in the Seventh Circuit and one district court in the Fifth Circuit have found that participant data is not a plan asset. The Seventh Circuit affirmed the *Northwestern University* decision without directly addressing the participant data claims, and the plaintiffs are likely to appeal to the Fifth Circuit the *Shell Oil Company* decision granting Fidelity's motion to dismiss. There are at least two cases currently pending (one 403(b) case and one 401(k) case) that allege participant data is a plan asset. Only time will tell whether similar allegations will be made in future excessive fee litigation. With the current legal landscape, plaintiffs will likely face an uphill battle with the participant data claims. While this issue plays out further in the courts, we recommend that plan fiduciaries review their own recordkeeping agreements and consider adding cross-selling restrictions if they want to preclude their recordkeepers from using participant data for cross-selling purposes in the future.

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

Even if participant data isn't a plan asset under ERISA, this litigation raises interesting questions about recordkeepers cross-selling non-plan products to plan participants.

[1] As of April 12, 2021, the case, *Sacerdote v. Cammack LaRhette Advisors, LLC*, No. 17 cv 8834 (S.D.N.Y.) (NYU 2) is pending, but is stayed until the Second Circuit decides *Sacerdote v. New York University* (NYU 1) No. 18-2707 (2d Cir.) (a related case that does not involve participant data claims).

[2] Participant data allegations were only in the proposed second amended complaint, which the district court denied leave to file.

[3] Also, although not raised as a claim in the complaint, plaintiffs in the Yale 403(b) excessive fee case made participant data and cross-selling an issue when their proposed expert included revenue earned from cross-selling in his calculations. *Vellali v. Yale University*, No. 3:16-cv-01345 (D. Conn. Dec. 4, 2020) (Dkt. 272).

[4] As of April 12, 2021, there are motions to dismiss pending in this case, *Berkelhammer v. ADP TotalSource Group, Inc.*, No. 2:20-cv-05696 (D.N.J.) (oral arguments scheduled June 2, 2021).

[5] As of April 15, 2021. *See also, Hughes v. Northwestern Univ.*, 141 S.Ct. 231 (2020) (inviting Acting Solicitor General to file a brief expressing the views of the United States).

[6] *Northwestern University*, 2018 WL 23p88118; Walsh, 266 F.R.D. 232; *Patient Advocates, LLC*, 316 F. Supp. 2d 46.

FIRM NEWS

Joe Faucher, **Brian Murray** and **Catherine Reagan** co-authored an article appearing in the Winter 2021 edition of the Journal of Pension Benefits. The article, "Attorney Fees in ERISA Benefits Litigation: Recent Cases," is the first in a two-part series regarding the law relating to awards of attorney fees in cases governed by the Employee Retirement Income Security Act.

Clarissa Kang and **Joe Faucher** have authored an article in the Spring 2021 newsletter of the ABA Tort Trial and Insurance Practice Section, Employee Benefits Committee. The article, "Supreme Court Gives Green Light to States to Regulate Pharmacy Benefit Managers," outlines key points and implications related to the Supreme Court's recent decision.

On April 7, **Joe Faucher** participated in a Strafford webinar panel discussion, *ERISA Litigation and Employee Stock Ownership Plans: The Evolving Landscape of Claims Against Fiduciaries*. This CLE webinar guided counsel on procedures and fiduciary responsibilities in employee stock ownership plan (ESOP) transactions and covered recent court rulings.

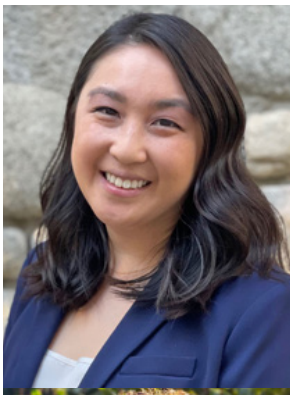
On April 20, **Tiffany Santos** was a panelist on the American Bar Association's Joint Committee on Employee Benefits' webinar titled *COBRA and Other Implications of Recent Stimulus Bills on ERISA Health Benefits*. This webinar provided an in-depth discussion of the COBRA subsidy under the American Rescue Plan Act of 2021 and the DOL's recent guidance implementing the Mental Health Parity and Addiction Equity Act.

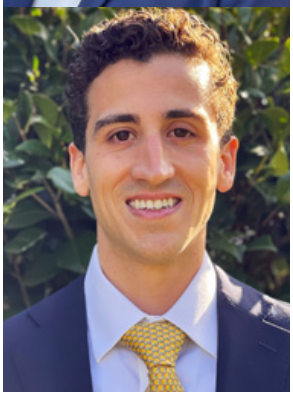
On April 21, **Marc Fosse** moderated a discussion regarding the JP Morgan Guide to Retirement at the Western Pension & Benefits Council's April chapter meeting.

On May 5, **Marc Fosse** will participate in a Strafford webinar panel presentation, *Employee Severance Agreements and Section 409A Deferred Compensation: Withstanding Heightened IRS Scrutiny*. This CLE webinar will provide counsel with guidance on structuring employee severance or separation agreements to comply with Section 409A's deferred compensation restrictions. The panel will discuss best practices for performing compliance self-audits and taking corrective action to remedy substantive or documentary failures.

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

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.

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

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.

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

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).

The Trucker ✦ Huss *Benefits Report* is published monthly to provide our clients and friends with information on recent legal developments and other current issues in employee benefits. Back issues of *Benefits Report* are posted on the Trucker ✦ Huss web site (www.truckerhuss.com).

Editor: Shannon Oliver, soliver@truckerhuss.com

In response to new IRS rules of practice, we inform you that any federal tax information contained in this writing cannot be used for the purpose of avoiding tax-related penalties or promoting, marketing or recommending to another party any tax-related matters in this *Benefits Report*.

Copyright © 2021 Trucker Huss. All rights reserved. This newsletter is published as an information source for our clients and colleagues. The articles appearing in it are current as of the date which appears at the end of each article, are general in nature and are not the substitute for legal advice or opinion in a particular case.

TRUCKER ✦ HUSS

Adrine Adjemian
aadjemian@truckerhuss.com
415-277-8012

Jahiz Noel Agard
jagard@truckerhuss.com
415-277-8022

Bryan J. Card
bcard@truckerhuss.com
415-277-8080

Nicolas D. Deguines
ndeguines@truckerhuss.com
415-277-8036

Lindsay R. Docto
ldocto@truckerhuss.com
415-277-8030

Joseph C. Faucher
jfaucher@truckerhuss.com
213-537-1017

J. Marc Fosse
mfosse@truckerhuss.com
415-277-8045

Angel Garrett
agarrett@truckerhuss.com
415-277-8066

Robert R. Gower
rgower@truckerhuss.com
415-277-8002

R. Bradford Huss
bhuss@truckerhuss.com
415-277-8007

Clarissa A. Kang
ckang@truckerhuss.com
415-277-8014

Sarah Kanter
skanter@truckerhuss.com
415-277-8053

T. Katuri Kaye
kkaye@truckerhuss.com
415-788-3111

Freeman L. Levinrad
flevinrad@truckerhuss.com
415-277-8068

Elizabeth L. Loh
eloh@truckerhuss.com
415-277-8056

Brian D. Murray
bmurray@truckerhuss.com
213-537-1016

Kevin E. Nolt
knolt@truckerhuss.com
415-277-8017

Yatindra Pandya
ypandya@truckerhuss.com
415-277-8063

Barbara P. Pletcher
bpletcher@truckerhuss.com
415-277-8040

Mary E. Powell
mpowell@truckerhuss.com
415-277-8006

Catherine L. Reagan
creagan@truckerhuss.com
415-277-8037

Dylan D. Rudolph
drudolph@truckerhuss.com
415-277-8028

Tiffany N. Santos
tsantos@truckerhuss.com
415-277-8039

Robert F. Schwartz
rschwartz@truckerhuss.com
415-277-8008

Charles A. Storke
cstorke@truckerhuss.com
415-277-8018

Jennifer Truong
jtruong@truckerhuss.com
415-277-8072

Nicholas J. White
nwhite@truckerhuss.com
415-277-8016

Jennifer L. Wong
jwong@truckerhuss.com
415-277-8077

PARALEGALS

Shannon Oliver
soliver@truckerhuss.com
415-277-8067

Susan Quintanar
squintanar@truckerhuss.com
415-277-8069

TRUCKER ✦ HUSS
A PROFESSIONAL CORPORATION
ERISA AND EMPLOYEE
BENEFITS ATTORNEYS

One Embarcadero Center, 12th Floor
San Francisco, California 94111-3617

15821 Ventura Blvd, Suite 510
Los Angeles, California 91436-2964

Tel: (415) 788-3111
Fax: (415) 421-2017
Email: info@truckerhuss.com

www.truckerhuss.com