No. 21-3290

IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

MARTIN J. WALSH,
Petitioner-Appellee

v.

ALIGHT SOLUTIONS LLC,
Respondent-Appellant.

On Appeal from the United States District Court
For the Northern District of Illinois, Eastern Division
Case No. 1:20-cv-2138
District Judge John F. Kness

BRIEF OF APPELLEE MARTIN J. WALSH, SECRETARY OF LABOR

SEEMA NANDA
Solicitor of Labor

G. WILLIAM SCOTT
Associate Solicitor for
Plan Benefits Security

THOMAS TSO
Counsel for Appellate and Special Litigation

ROBIN SPRINGBERG PARRY
Senior Regulatory Attorney

RACHEL UEMOTO
Trial Attorney
Plan Benefits Security Division
Office of the Solicitor
U.S. Department of Labor
200 Constitution Ave. NW, N-4611
Washington, DC 20210
(202) 693-5600

TABLE OF CONTENTS

TABLE OF CONTENTS-continued

TABLE OF AUTHORITIES

Federal Cases:

Federal Cases-continued:

Federal Cases-continued:

Federal Cases-continued:

Federal Cases-continued:

Federal Cases-continued:

Federal Cases-continued:

State Cases:

State Cases-continued:

Federal Statutes:

Title 5, Government Organization and Employees

Title 15, Commerce and Trade

Employee Retirement Income Security Act of 1974, (Title I)
as amended, 29 U.S.C. 100 et seq.,

Miscellaneous:

QUESTIONS PRESENTED

The Employee Retirement Income Security Act (ERISA) entrusts the Secretary of Labor (Secretary) with the "duty of protecting the individual beneficiaries of [benefit] programs [and] an even stronger and paramount obligation to protect the very integrity, heart and lifeline of the program itself." *Sec'y of Labor v. Fitzsimmons*, 805 F.2d 682, 692–93 (7th Cir. 1986). To fulfill this duty, ERISA section 504(a)(1), 29 U.S.C. § 1134(a)(1), grants the Secretary "the power, in order to determine whether any person has violated or is about to violate any provision of this subchapter or any regulation or order thereunder . . . to make an investigation, and in connection therewith to require the submission of reports, books, and records[.]" "Alight currently provides recordkeeping services to ERISA-covered retirement or benefits plans (including defined benefits, defined contribution, and health administration plans) for over 750 clients and over 20.3 million plan participants." R. 15-1 ¶ 10 (Dodson Decl.). Services include maintaining cybersecurity for records. R. 35 ¶¶ 10-12. Plan clients entrust important plan information to Alight. R. 30 at 3. No one can dispute that cybersecurity breaches pose a serious risk to plans and their participants. *See* R. 58 at 3 (citing GAO-21-25, *Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement*

Plans, at 25 (Feb. 11, 2021) and DOL guidance). And no one can dispute that cybersecurity events can result in serious harm to plan participants. Br. at 33 (recognizing GAO identified cybersecurity protection as a "compelling need," citing GAO report). Yet, despite these significant risks of harm to plans and participants, directly implicating the very integrity of plans, Alight urges this court to overrule the district court's findings and conclusions that support subpoena enforcement to obtain plan records from a major provider of cybersecurity and record-keeping services to ERISA-covered plans. This appeal presents these three questions:

1. Did the District Court correctly conclude that the DOL met its burden of establishing that the Secretary has authority to issue the Subpoena for records concerning ERISA plans and that the Subpoena is not too indefinite and seeks information reasonably relevant to the investigation, after learning that Alight suffered a cybersecurity breach which potentially harmed ERISA plan participants whose records are maintained by Alight?

2. Did the District Court correctly find that Alight failed to show that its burden of compliance outweighed the relevance of the requests to the Secretary's investigation of potential ERISA violations?

3. Did the District Court correctly deny Alight's request for a protective order where the PII and confidential information are protected

from government disclosure by FOIA, will not be presented into evidence, and are necessary for the Secretary's investigation?

BACKGROUND

On July 30, 2019, the U.S. Department of Labor's Employee Benefit Security Administration (EBSA) opened an investigation of Alight. Alight "is a worldwide healthcare and retirement benefits administration and cloud-based human resources services company[.]" R. 15-1 ¶ 4. "Alight has served as one of the leading providers of benefits administration, cloud-based human resources and related financial solutions in the industry." *Id.* "[Its] clients entrust Alight with highly sensitive information about their company and employee benefit plans[.]" *Id.* ¶ 5. "Alight provides recordkeeping services for employee benefit plans, including plans subject to the Employee Retirement Income Security Act ("ERISA") ("ERISA Plans") and plans that are not subject to ERISA." *Id.* ¶ 8. Alight provides recordkeeping, administrative, and consulting services to over 750 client plans covered by ERISA that serves "over 20.3 million plan participants." R. 15-1 ¶ 10. Alight provides cybersecurity services to ERISA plans. R. 35 ¶¶ 10-12.

Maintaining cybersecurity of those records for ERISA plan participants is a significant part of Alight's business and its known risks.

"As a leader in cloud-based and remote outsourcing, the security and confidentiality of client data is of paramount importance to Alight." R. 15-1 ¶ 5. Alight publicly acknowledged a "known risk" that "cyber-attacks and security vulnerabilities and other significant disruptions in the Company's information technology systems and networks that could expose the Company to legal liability, impair its reputation or negative effect on the Company's results of operations."[1] Among the "significant challenges and risks" Alight described is the "[i]mproper access to, misappropriation, destruction or disclosure of confidential, personal or proprietary data as a result of employee or vendor malfeasance or cyber-attacks [which] could result in financial loss*, regulatory scrutiny*, legal liability or harm to our reputation."[2] (emphasis added).[3] Alight recognizes plan participants can be

[1] Alight, Form 10-Q, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001844744/4d890b30-1b6a-498a-b163-f99fc4dd78eb.pdf.; *see Petrobras Am., Inc. v. Samsung Heavy Indus. Co., Ltd.*, 9 F.4th 247, 255 (5th Cir. 2021) (using judicial notice to infer knowledge of the statements in the documents).

[2] Exhibit 4 to Alight's motion to dismiss, Barnett v. Abbott Laboratories, No.1:20-cv-02127 (N.D. Ill. Feb. 8, 2021).

[3] Live matters related to cybersecurity involving Alight include: "(1) *Bartnett v. Abbott Laboratories*, (N.D. Ill. Case No. 20-cv-02127); (2) *Berman v. Estee Lauder, Inc.* (N.D. Cal. Case No. 3:19-cv-06489); (3) two United States Department of Justice ("DOJ") subpoenas concerning criminal proceedings against third parties; and (4) a pending request from the Delaware Department of Justice ("DDOJ")." R. 32-1 at 6.

harmed by improper disclosure of its information through cyber-attacks. *See* Br. at 51-52 ("plan participant PII is highly confidential and warrants protection from disclosure through redaction, which protects plan participants from potential embarrassment and identity theft risks created through risks of inadvertent disclosures, cybersecurity hacking, and public filings in potential future litigation.").

The security of plan information is not a new area of concern for the Secretary. DOL regulations require assurances that "[t]he electronic recordkeeping system has reasonable controls to ensure the *integrity*, accuracy, authenticity and reliability of the records kept in electronic form[.]" 29 C.F.R. § 2520.107-1 (emphasis added) (went into effect in 2002); *see also* 29 C.F.R. §§ 2520.104b-31(e)(3), (k)(4) (requiring the plan administrator to protect participant information stored on websites or sent to participants via email) (went into effect in 2020); 29 C.F.R. § 2520.104b-1(c) (ensuring protection of participant information) (electronic disclosure requirements went into effect in 1997). In recognition of the grave dangers cyberthreats pose to plan benefits and retirement security, the Department issued guidance to "recordkeepers" (like Alight), and to plans and

recordkeepers on "cybersecurity best practices,"[4] noting that "plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."[5] Given this background, Alight cannot feign surprise that DOL will seek to understand how plans and their providers protect the confidentiality of plan participant information in light of known risks related to cybersecurity.

This interest in Alight is not abstract. EBSA discovered that Alight processed unauthorized distributions of ERISA plan benefits due to cybersecurity breaches in its ERISA plan clients' accounts and failed to disclose those breaches and unauthorized distributions to those plan clients for months, and so EBSA began investigating Alight to determine whether any person, including Alight or any fiduciaries serving its clients, "has violated or is about to violate any provision of Title I of ERISA or any regulation or order promulgated thereunder." 29 U.S.C. § 1134(a)(1);

---

[4] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf; https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity.

[5] *Id*. EBSA's investigation may include "review of an effective audit program," including an assessment of whether a third party has reviewed a party's cybersecurity practices in order to mitigate potential harm to plan participants. https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

Loggins Declaration (Exh. A to Sec'y Opp. to Mot. to Stay, Dkt. 13). As part of its investigation, EBSA determined it was essential to obtain information from Alight, and issued an Administrative Subpoena *Duces Tecum* (Subpoena) on November 5, 2019, as authorized by ERISA section 504(a)(1), 29 U.S.C. § 1134(a)(1). The Subpoena calls for all documents in Alight's possession, custody, or control in response to 32 inquiries, and specifies that unless otherwise noted, the time period covered by the Subpoena is from January 1, 2015, to the date of production. R. 25 at 2. Over the next six months, the Department attempted to negotiate with Alight over the production, but Alight failed to produce most documents.

The underlying dispute consists of routine discovery issues eventually presented to and resolved by the district court within the bounds of its discretion. Without need to delve deeper into the back-and-forth, in its various filings, Alight admits several important points for this appeal. First, both sides conferred and accommodated on various points. Loggins Decl. at 5 (R. 1-1) (describing 30-day extension EBSA granted, and agreement for rolling production after objection); Reply Mem. at 9-12 (R. 18) (describing modifications to the Subpoena). Second, both sides, as is commonplace, disagreed with some representations from the other side. Third, Alight relied on various excuses to delay production, some of which are no longer

valid or, if accepted, would permanently exempt Alight from complying with any administrative subpoena. *E.g.,* R. 32-1 at 3 (refusing to comply because, at the time, Alight must "serve its clients during open enrollment"); *id.* (refusing to comply because Alight's "ongoing responsibility to ensure the security of Alight's clients' and their participants' data and assets"). Fourth, Alight refused to produce further documents unless the Secretary proved, before investigating further, that plan clients had reported losses in public reports. Loggins Decl. at 8 (R. 1-1) (describing how Alight refused to produce unless "the plan 'ha[d] a loss, whether or not reimbursed by the plan's fidelity bond, that was caused by fraud or dishonesty.'").

Alight also concedes it receives and secures important *plan* information from its plan clients, "including: names, contact information (including home address, phone numbers, and e-mail addresses), social security numbers, asset information, investment information, beneficiary information, contribution levels[,]" R. 30 at 3, "information about their company and employee benefit plans including: total plan asset values, company contributions, the structure of company benefit plans, benefit plan designs, plan costs[.]" R. 15-1 at ¶ 5. Such information seems highly relevant to any investigation into a plan and its service providers, like Alight.

Finally, Alight concedes that the incidents described in the Department's factual basis underlying its Subpoena *would* be suitable for investigation to benefit the plans and participants: "[i]f the DOL's allegations are correct, it is in everyone's best interest – the plan participant(s), the ERISA Plan(s), the DOL and Alight – for Alight to investigate and remediate the issues as soon as possible." R. 35 at 9. While recognizing the Secretary should investigate cybersecurity issues impacting plans, Alight does not want to provide any more information beyond limited, redacted documents for a few discrete incidents. Alight contends it should only have to provide documents "surrounding the specific incidents that prompted the DOL's investigation." *Id*.

On April 6, 2020, the Secretary petitioned the district court to enforce the Subpoena. The district court granted the petition on October 28, 2021. Alight appealed that decision and filed an opening brief on January 19, 2022. On January 24, the district court denied Alight's motion for a stay pending appeal. R. 59. After the district court issued its order denying the stay, the Secretary inquired whether Alight intended to comply with the Subpoena and the district court's orders. In the event that Alight chose to disobey the district court's orders, the Secretary notified Alight that he would file a motion with the court. Alight then filed the motion to stay

subpoena enforcement in this Court on January 27, 2022, and the Secretary filed the motion in opposition to the stay ("Opp.") on February 10, 2022. This Court denied the motion to stay on February 15, 2022. Dkt. 14.

SUMMARY OF ARGUMENT

1. The district court correctly held that the Secretary was authorized by ERISA to issue the Subpoena. EBSA issued the Subpoena after learning that Alight suffered cybersecurity breaches that caused potential harm to its ERISA plan clients' accounts. First, the district court correctly held that both the text of the statute and controlling case law support the Secretary's authority to investigate without first being required to identify a violation. In ERISA section 504(a)(1), Congress gave the Secretary the power to investigate "*in order to determine* whether any person has violated or is about to violate ERISA," and thus the Secretary is not required to determine that a violation occurred *before* he subpoenas documents. Well-established case law holds that subpoena enforcement proceedings are not forums to litigate questions of coverage of federal statutes.

Second, Alight waived its argument that cybersecurity is outside the Secretary's investigatory reach, as it failed to present that argument to the district court in the briefs responding to the petition for enforcement. Further, nothing in ERISA insulates electronic recordkeeping for ERISA

plans, which typically store data electronically and hold trillions in assets, from regulatory oversight by the Secretary. Given that cybersecurity breaches can harm the security of ERISA plans, that fiduciaries must ensure that plan assets and information are secure, and that plan service providers such as Alight manage plan assets and information, cybersecurity is a critical aspect of plan benefit security, and the Secretary is well within his authority to investigate cyberbreaches.

Third, even if one assumes that Alight is not a fiduciary, the district court correctly held that the Secretary is authorized by ERISA to investigate non-fiduciaries. As recognized by the Supreme Court and this Court, the statute broadly permits the Secretary to seek information from anyone who has information relevant to a potential ERISA violation, regardless of whether they themselves are fiduciaries. ERISA section 504(a)(1) gives the Secretary broad statutory power to investigate, "in order to determine whether *any* person has violated or is about to violate *any* provision of this title or *any* regulation or order . . ." The plain text precludes the limit that Alight seeks, and indeed the Supreme Court has recognized the Secretary's authority to identify, seek equitable remedies from, and penalize non-fiduciaries for violations. Alight, as a service provider to a plan, is a "party in interest" under ERISA section 3(14), and its actions concerning ERISA

plans may cast light on its own liability as a party-in-interest or as a functional fiduciary, or on breaches by its clients that are fiduciaries. Multiple cases support subpoenas to non-fiduciaries.

2. The district court properly assessed the Secretary's Subpoena requests and found they are sufficiently definite. The court reviewed each of the specific requests in the 32 paragraphs of the Subpoena and the modifications made by the Secretary during litigation, and correctly found that none of them were too indefinite. The Subpoena specifically requested information within statutory bounds and requested only that information which the Secretary deems necessary to determine compliance with the obligations ERISA imposes on plan fiduciaries and service providers.

The district court correctly found, after weighing the evidence, that Alight failed to carry its heavy burden of showing that the Subpoena is unduly burdensome when balanced against the relevance to the investigation of the documents requested. The district court opinion shows that the court used the correct test, first explicitly determining that the Subpoena requests are "reasonably relevant to the investigation," because "records identifying specific plans as well as records of the plans themselves fall within the scope of a proper ERISA investigation." Only after making the prerequisite determinations that the Subpoena was within the Secretary's authority, not

too indefinite, and requested information reasonably relevant to the investigation, did the court move to the next test, weighing the burden on Alight against the relevance of the Subpoena's request. As this Court has held, a district court's finding of reasonable relevance cannot be overturned absent a showing that the underlying factual determinations are clearly erroneous or the ruling was an abuse of discretion. Alight can make no such showing. The district court then weighed the burden on Alight against the relevance of the documents to the investigation, and properly held that the balance weighed in favor of the Secretary. The court correctly found that Alight had the high burden of proof to show that the Subpoena is unduly burdensome such that it would outweigh the relevance of the documents, and given the presumption that subpoenas should be enforced, it failed to convince the factfinder. Subpoena compliance always requires some effort, but inconvenience is not enough to quash a subpoena. The court found that Alight failed to prove that the Subpoena is *unduly* burdensome such that it would threaten the normal operation of its business, the standard used in numerous cases.

3. In denying the protective order, the district court correctly found that the Secretary is entitled to unredacted documents that contain Personal Identifiable Information ("PII"), confidential settlement agreements, and

client-identifying information, all of which are necessary in order to fully investigate for potential ERISA violations. The court properly found that Alight did not show "good cause" for an order limiting the Subpoena to "de-identified" data, and the court properly weighed and correctly dismissed Alight's concerns about disclosure of its protected information by the government. Alight has not shown that the district court abused its discretion in its ruling. As the court found, confidential information is protected under the Freedom of Information Act (FOIA), and Alight showed no reason why the Secretary should not be entitled to receive records including such information.

Further, disclosure of settlement agreements to the Secretary will not harm Alight or its clients. Alight's argument that settlement agreements should remain confidential in order to encourage settlements speaks to the Federal Rules of Evidence. However, numerous cases hold that confidentiality clauses cannot shield agreements from discovery categorically, and in fact courts have found that the Secretary has an important role in examining ERISA settlements to determine if they serve participant and public interests.

Finally, the information Alight asks to de-identify, such as client names, is necessary for the Secretary to identify potential ERISA violations

and the individuals or entities that might be responsible for harming plan participants. Allowing companies like Alight to redact or withhold key information would leave the Secretary in the dark and unduly limit or nullify his investigatory authority. Therefore, Alight could not show good cause to redact the information requested, and the district court did not abuse its discretion in so holding.

ARGUMENT

Subpoena enforcement proceedings "are designed to be summary in nature" and "a district court's subpoena enforcement function is narrowly limited[.]" *E.E.O.C. v. Aerotek, Inc.*, 815 F.3d 328, 333 (7th Cir. 2016). "As long as the investigation is within the agency's authority, the subpoena is not too indefinite, and the information sought is reasonably relevant, the district court *must* enforce an administrative subpoena." *E.E.O.C. v. United Air Lines, Inc.*, 287 F.3d 643, 649 (7th Cir. 2002) (emphasis added). As the district court correctly found, R. 25 at 3-5, the Secretary satisfied these requirements. The court noted that courts "may modify or exclude portions of a subpoena only if the employer carries the difficult burden of showing that the demands are unduly burdensome or unreasonably broad." *Id.* at 5. The district court then weighed the burden on Alight, "which the Court does not take lightly," and found that it needed to weigh the relevance of the

requests against Alight's burden, and that the balance favored the Department's requests, particularly considering the presumption that subpoenas should be enforced. *Id*. The court then noted that under controlling precedent, Alight needed to show not merely that the Subpoena is burdensome, but that it is *unduly* burdensome. *Id*. The court found that in this case, the relevance outweighed the burden on Alight, and the burden did not justify refusing to enforce the Subpoena. *Id*. at 5-6; *see Aerotek*, 816 F.3d at 333.

Such decisions are "within the sound discretion of the trial court and should only be reversed for abuse of discretion." *Aerotek*, 816 F.3d at 333 (holding, under "these deferential standards," that district court properly enforced EEOC's subpoena); *E.E.O.C. v. Quad/Graphics, Inc.*, 63 F.3d 642, 645 (7th Cir. 1982) (district court's decision to enforce agency subpoena generally is reviewed deferentially); *see generally McLane Co. v. E.E.O.C.*, 137 S. Ct. 1159, 1168 (2017). As the Supreme Court recognized in *McLane*, appellate courts only review for abuse of discretion: "whether the evidence sought is relevant to the specific charge before it or whether the subpoena is unduly burdensome in light of the circumstances." 137 S. Ct. at 1167-68. "Abuse of discretion is a highly deferential standard. 'Abuse of discretion means a serious error of judgment, such as reliance on a forbidden factor or

failure to consider an essential factor.'" *In re Veluchamy,* 879 F.3d 808, 823 (7th Cir. 2018). The "abuse of discretion" standard "'means something more than [this Court's] belief that [it] would have acted differently if placed in the circumstances confronting the district judge.' . . . For an abuse of discretion to occur, the district court's decision must strike [this Court] as fundamentally wrong." *Johnson v. J.B. Hunt Transp., Inc.*, 280 F.3d 1125, 1131 (7th Cir. 2002). In short, the circuit court "will affirm unless no reasonable person could agree with the district court." *Nelson v. Apfel*, 210 F.3d 799, 802 (7th Cir. 2000). The District Court properly weighed the facts before it and applied the law, and did not abuse its discretion.

I. The District Court Correctly Found that the Secretary Was Authorized to Issue the Subpoena for Records Concerning ERISA Plans.

Alight makes three arguments that the Secretary lacks authority to issue the Subpoena, all contrary to the plain text of the statute. First, it incorrectly contends that the Secretary must first establish the requested information relates to conduct that violates ERISA before enforcing a subpoena for records. Br. at 31. Second, it wrongly argues that the permissible scope of investigations of ERISA violations excludes cybersecurity. Third, it argues -- notwithstanding established precedent holding otherwise -- that only fiduciary conduct may be investigated. As

discussed below, all contentions are flatly wrong in light of the clear statutory language.

A. The District Court Correctly Ruled that the Secretary is Not Required to Establish a Violation Before Investigating

Alight concedes it serves ERISA-governed plans and keeps their records. *E.g.,* Br. at 4. As a matter of law, the statute plainly empowers the Secretary to "require the submission" of records from Alight to help determine if "any person" related to the plans Alight serves has violated ERISA or its regulations. ERISA section 504(a)(1), 29 U.S.C. § 1134(a)(1).

Instead of this plain-text reading of the statute, Alight twists the statutory text to conclude that "[t]he Secretary's subpoena authority is thus limited to investigations of alleged conduct that, if proven, could constitute a past or potential violations of those ERISA provisions." Br. at 31 (complaining the Secretary has provided insufficient information justifying the Subpoena). Alight essentially seeks a preliminary ruling on whether it could be found liable for an ERISA violation before it will comply with the Subpoena. There is no basis for such a rule, and it contravenes not only the text, but the controlling case-law.

First, the argument disregards the statutory text. Alight's argument has no basis in the text it cites. Section 504(a)(1) provides that "the Secretary shall have the power, in order to determine whether any person has

violated or is about to violate any provision" of Title I of ERISA or corresponding DOL regulation, "to make an investigation." 29 U.S.C. § 1134(a). Section 504(c) applies "[f]or the purposes of any investigation provided for" in Title I of ERISA. 29 U.S.C. § 1134(a)(1), (c). Neither provision limits the Secretary's subpoena authority in the manner Alight contends. *Cf. Cent. States, Se. & Sw. Areas Pension Fund v. Cent. Transp., Inc.*, 472 U.S. 559, 578 (1985) ("ERISA grants the Secretary of Labor broad investigatory powers" under section 504, 29 U.S.C. § 1134); *Chao v. Local 743, Int'l Bhd. Of Teamsters, AFL-CIO*, 467 F.3d 1014, 1017 (7th Cir. 2006) (upholding enforceability of subpoena and referring to Secretary's "broad authority to investigate"). Clearly, the information provided in the investigation is to be used for the *agency,* not the *court*, to determine in the first instance whether any person has violated ERISA. (Should the Secretary determine there is such a violation, the Secretary may then bring an enforcement action in district court to compel the person to remedy the violation.) In the grant of subpoena power, Congress specified "the Secretary shall have the power, *in order to* determine whether any person has violated [ERISA]," indicating that obtaining documents via an investigation would then inform the Secretary in making that determination. 29 U.S.C. § 1134(a)(1).

The Secretary can thus investigate "to *determine whether* any person has violated or is about to violate" ERISA. *Id*. The Secretary is not required to determine a violation occurred or is about to occur *before* he subpoenas documents. Alight's contention is similar to arguments for grafting non-statutory limits to the Department's investigative authority that were rejected in *Donovan v. Shaw*, 668 F.2d 985, 990 (8th Cir. 1982). The Eighth Circuit recognized that the Secretary's power to investigate under section 504(a)(1), unlike other section 504 provisions, does not require "reasonable cause" to believe a violation occurred before requesting records, let alone some prerequisite to establish violations.[6] *Id.*; *accord Donovan v. Nat'l Bank of Alaska*, 696 F.2d 678, 684 (9th Cir. 1983); *see also Local 743, Int'l Bhd. of Teamsters*, 467 F.3d at 1018-19 (applying similar rationale to the LMRDA). The district court correctly concluded that the Secretary has authority to investigate without requiring the Secretary to identify a violation. R. 25 at 3. Contrary to Alight's framing of this case, the boundaries of the Secretary's investigative authority do not turn on some prior reasonable cause showing that the records relate to conduct that violates ERISA.

[6] Like in *Shaw,* 668 F.2d at 987 & n.2, the Subpoena requests records under section 504(a)(1), see Exhibit C to the Motion for Stay.

Second, established case-law supports this reading. "It is well settled that a subpoena enforcement proceeding is not the proper forum in which to litigate the question of coverage under a particular federal statute." *Shaw*, 668 F.2d at 989. Courts also "will not . . . turn a summary subpoena-enforcement proceeding into a mini-trial by allowing [a party] to interpose defenses that are more properly addressed at trial." *CSG Workforce Partners, LLC v. Watson*, 512 F. App'x 830, 833 (10th Cir. 2013) (unpublished). Alight wants to transform subpoena enforcement into a "mini-trial" on whether the Secretary can establish a violation before receiving the majority of the subpoenaed documents, on how and whether cybersecurity breaches constitute an ERISA violation, and on whether their alleged non-fiduciary status means they are not covered by the statute. *See* Br. at 30-36.

The District Court correctly held that there was no legitimate barrier to enforcing the Subpoena simply because it did not state what specific violation was being investigated. "There is, likewise, no jurisdictional basis (as Respondent argues) to decline enforcement of a subpoena merely because the Subpoena does not 'reflect what alleged actual or imminent ERISA violation is under investigation or how [the Respondent's] business records are relevant to any such investigation.'…The relevant statute

contains no such requirement, see 29 U.S.C. § 1134, and Respondent has not directed the Court to any separate authority for such a requirement." R. 25 at 3, n.2.

B. The Secretary is Well Within His Authority to Investigate Threats to Plan Information and Benefits, Including Cybersecurity Dangers

Even if Alight were correct that the Secretary must establish some showing that the Secretary is investigating a violation, which he need not, Alight's argument that the Secretary cannot investigate cybersecurity incidents because cybersecurity is outside the Department's regulatory scope is erroneous. Br. at 31. First, nowhere in the briefs below in response to the petition for enforcement does Alight present this argument to the district court. Consequently, this argument is waived. *See Wheeler v. Hronopoulos*, 891 F.3d 1072, 1073 (7th Cir. 2018) ("Failing to bring an argument to the district court means that you waive that argument on appeal.").

Although the Court should decline to reach the issue, the integrity of plan recordkeeping systems is squarely within the Department's regulatory scope. Pursuant to ERISA section 404, fiduciaries "shall discharge [their] duties with respect to a plan solely in the interest of the participants and beneficiaries . . . with the care, skill, prudence, and diligence" of a prudent person in similar circumstances. 29 U.S.C. § 1104(a). The obligation to act

in the interest of participants and beneficiaries is commonly referred to as the duty of loyalty, *Cent. States*, 472 U.S. at 570, and the obligation to act prudently is referred to as the duty of prudence. The Department has a responsibility to ensure that plan fiduciaries and the plan's service providers satisfy these duties. In an increasingly virtual world where most records are maintained electronically, these duties require fiduciaries to ensure that ERISA plan records are maintained safely so as to protect the participants' and beneficiaries' information and assets. When fiduciaries employ parties such as recordkeepers or other entities to service plans, fiduciaries are obligated to monitor these providers to uphold these duties and the providers cannot knowingly participate in violations.

The dangers of cybersecurity breaches and their potential consequences, including loss of assets necessary to pay plan benefits and exposure of sensitive data, are well-known.[7] Even Alight acknowledges that cybersecurity breaches threaten the integrity of plan recordkeeping systems. *See, e.g.*, Br. at 33.[8] The effect of cybersecurity breaches can be enormous.

---

[7] U.S. Gov't Accountability Office, GAO-21-25, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans, at 15-17 (Feb. 11, 2021), https://www.gao.gov/assets/gao-21-25.pdf.

[8] Alight has been involved in incidents related to retirement systems, *see* https://www.ers.ga.gov/identity-information.

Alight alone provides electronic recordkeeping to ERISA plans that provide benefits to over 20 million plan participants. Br. at 41. ERISA-covered plans and their recordkeepers, like Alight, typically store data electronically and collectively hold over $12 trillion in assets, as well as personal data relating to more than 150 million plan participants and beneficiaries.

Contrary to Alight's suggestion, nothing in ERISA insulates cybersecurity from regulatory oversight and review, or from the fiduciary obligations of prudence, loyalty, and avoidance of prohibited transactions. Given the potential consequences to plan accounts of cybersecurity breaches, in the form of misappropriation of assets, breaches of confidentiality, identity theft, etc., cybersecurity is a critical aspect of plan benefit security. Fiduciaries must ensure plans' assets and information are secure, and this responsibility includes the fiduciary obligation to carefully select and monitor plan service providers, who manage plan assets and information. *See Chao v. Merino*, 452 F.3d 174, 182 (2d Cir. 2006) ("If a fiduciary was aware of a risk to the fund, he may be held liable for failing to investigate fully the means of protecting the fund from that risk.").

The ways cybersecurity failures can threaten plan assets is illustrated by a case in which Alight acted as recordkeeper, *Bartnett v. Abbott Labs*, 492 F.Supp.3d 787 (N.D. Ill. Oct. 2, 2020). In this cyberbreach case, a

retirement plan participant alleged that $245,000 of her retirement account was stolen when an unknown person breached her retirement account via the Abbott Benefits website and the Abbott Benefits Center (a customer service call center), both operated by Alight. *Id*. at 792-94. The theft was allegedly carried out by a person using the "Forgot Password" option online and making phone calls to the Benefits Center asking how to transfer funds to a new bank account, reportedly without being asked security questions. *Id*. at 792-94, 798-99 (allowing claim against Alight to proceed).

The Department has broad authority to investigate whether fiduciaries and service providers (whether as parties in interest[9] or as functional fiduciaries)[10] have violated ERISA, including whether they have imprudently or disloyally exposed plan participants to cybersecurity breaches, and Alight points to no authority to the contrary. Only after an investigation can the Department determine whether plan fiduciaries have selected and monitored such service providers with prudence and loyalty as

[9] ERISA § 3(14) ("[P]roviding services to [a] plan" makes Alight a party in interest). 29 U.S.C. § 1002(14).

[10] Without relevant documents, the Secretary cannot yet state with certainty whether Alight is or is not a functional fiduciary. *See Hecker v. Deere & Co.*, 556 F.3d 575, 583 (7th Cir. 2009) (explaining functional fiduciary status); *see generally Bartnett*, 492 F. Supp. 3d at 798-9 (finding plausible claim of Alight's fiduciary status).

ERISA requires, find whether the arrangements with the service providers are "reasonable" as required by section 408(b)(2), identify the relevant plans and plan fiduciaries, assess the fiduciary status of the recordkeepers, determine the scope of any breaches under section 404 and 406, and ascertain losses.

The Department has long recognized the grave dangers cyberthreats pose to plan benefits and retirement security. The Department recently issued guidance to "recordkeepers" (like Alight), and to plans and recordkeepers on "cybersecurity best practices," noting that "plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."[11] Long before the most recent cybersecurity guidance, the Department issued regulations requiring the security of electronic recordkeeping for plans. *See, e.g.*, 29 C.F.R. § 2520.107-1 (2002) (requiring that "[t]he electronic recordkeeping system has reasonable controls to ensure the *integrity*, accuracy, authenticity and reliability of the records kept in electronic form[.]") (emphasis added); 29 C.F.R. § 2520.104b-1(c) (1997) (requiring that electronic recordkeeping and disclosure "[p]rotects the confidentiality of

[11] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf; https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity.

personal information relating to the individual's accounts and benefits (e.g., incorporating into the system measures designed to preclude unauthorized receipt of or access to such information by individuals other than the individual for whom the information is intended)").[12]

As mentioned above, this obligation derives from ERISA's statutory duties of loyalty and prudence, 29 U.S.C. § 1104(a), sourced from the law of trusts. *E.g., Cent. States,* 472 U.S. at 570 (1985). For example, as Restatement (Third) of Trusts § 78 (2007) notes, "[i]ncident to the duty of loyalty . . . is the trustee's duty to preserve the confidentiality and privacy of trust information from disclosure to third persons." *Id.*; *accord In re Estate of Miller*, 18 A.3d 1163, 1172 (Pa. Super. Ct. 2011); *Zastrow v. Journal Commc'ns, Inc.*, 718 N.W.2d 51, 60 (Wis. 2006); *compare F.T.C. v.*

---

[12] The Secretary continued to further develop cybersecurity guidance throughout the last decade, including reviewing detailed reports from the ERISA Advisory Council. https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf "The 2016 Council's work built upon the 2011 ERISA Advisory Council's ('2011 Council') prior work, which examined privacy and security issues affecting employee benefit plans. The 2011 Council report included, among other things, recommendations with respect to guidance and educational materials for plan sponsors, plan participants and vendors. In addition, the 2015 ERISA Advisory Council ('the 2015 Council') devoted some time to the topic of cybersecurity. Leveraging the previous Councils' work, the 2016 Council focused specifically on outlining elements of cyber risk management strategies that can be scaled, or adjusted, based on sponsor and plan size, type, resources and operational complexity." *Id.*

Wyndham Worldwide Corp., 799 F.3d 236, 246–47 (3d Cir. 2015) (affirming FTC's ability to use statutory authority to investigate cybersecurity incidents). ERISA fiduciaries and plan service providers must ensure these fiduciary duties of loyalty and prudence are upheld. *See, e.g., Godfrey v. Greatbanc Tr. Co.*, No. 18 C 7918, 2019 WL 4735422, at *7 (N.D. Ill. Sept. 26, 2019) (finding plausible allegations that non-fiduciaries knowingly participated in a fiduciary breach). Cybersecurity concerns fall within statutory and regulatory obligations to protect plan information and the Department must ensure these obligations are met. As Alight concedes, possible past incidents are important to the plans, and therefore the Secretary has to serve an important public interest to *prevent* future cybersecurity incidents from harming plan assets and information and to assess the level of security involved. Courts have noted that "[t]he Secretary protects the public interest in 'prevent[ing] those who have engaged in illegal activity from causing loss to *any* future ERISA plan participants.'" *Id.* (quoting *Donovan v. Cunningham,* 716 F.2d 1455, 1462 (5th Cir. 1983)).

C. The District Court Correctly Held that ERISA Does Not Limit the Secretary's Authority to Investigate to Fiduciaries Only

The Secretary has broad statutory "power, in order to determine whether *any* person has violated or is about to violate *any* provision of this

title or *any* regulation or order . . . to make an investigation, and in connection therewith to require the submission of reports, books, and records[.]" 29 U.S.C. § 1134(a)(1) (emphasis added). Alight argues that it is not a fiduciary and baldly contends that the Secretary's authority to investigate is limited to fiduciaries, a limit that does not exist in section 504(a)(1). Mot. at 11-12. The plain text endows the Secretary with power to determine if "any person has violated or is about to violate" ERISA and investigate and obtain any records "in connection therewith." 29 U.S.C. § 1134(a). *See, e.g., Nat'l Bank of Alaska*, 696 F.2d at 684 (enforcing ERISA subpoena to financial recordkeeper and recognizing financial records may assist in "determining whether any person is violating or has violated" ERISA). "[T]he word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'" *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 219 (2008) (citations omitted). "Any person" in this context includes not just fiduciaries but also parties in interest, who can also be held liable for violating ERISA. Moreover, "the meaning of the phrase 'in connection with' should be construed expansively." *United States v. Wyatt*, 102 F.3d 241, 247 (7th Cir. 1996). Thus, whether Alight is a fiduciary, a party in interest, or some other person who can violate ERISA or whether it merely

has information about someone violating ERISA, the Secretary has authority to seek information from Alight.

The district court correctly held that that the plain text precludes the limit Alight claims. R. 25 at 3. ("Respondent's argument that the Subpoena power only extends to entities classified as 'fiduciaries' . . . is not supported by the text of the statute."). Alight does not attempt to analyze the text of the statute to challenge this conclusion, providing no basis to overturn that ruling. Indeed, the Supreme Court recognized the Secretary's responsibility to identify, seek equitable remedies from, and penalize non-fiduciaries for violations. *Harris Tr. & Sav. Bank v. Salomon Smith Barney, Inc.*, 530 U.S. 238, 249 (2000). The Secretary routinely investigates non-fiduciary parties in interest to plans, such as recordkeepers and third-party administrators, determining whether they are knowing participants in fiduciary breaches, functional fiduciaries, or can cast light on breaches by fiduciaries. Alight is such a "party in interest" under ERISA section 3(14) because it is "providing services to [a] plan." 29 U.S.C. § 1002(14)(B). "Congress defined 'party in interest' to encompass those entities that a fiduciary might be inclined to favor at the expense of the plan's beneficiaries." *Harris Tr.*, 530 U.S. at 242.

Courts uniformly rejected similar claims that the Secretary's authority to investigate is limited to ERISA fiduciaries. "The determination of

whether [an investigated entity] is an ERISA fiduciary or de facto [functional] fiduciary or may have party in interest liability under ERISA and/or whether any of [its] clients have violated ERISA are determinations for the Secretary to make in the first instance, not [the] Court." *Garlick & Tack Inc. v. Solis*, No. SAVC 13-0047, 2013 WL 12153508, at *1 (C.D. Cal. Mar. 27, 2013). This is because "'[a] party may not defeat agency authority to investigate a claim that could be a defense if the agency subsequently decides to bring an action against it.'" *Id*. (citing *E.E.O.C. v. Fed. Express Corp.*, 558 F.3d 842, 848 (9th Cir. 2009)); *see also Brock v. United Maint. Serv., Inc.*, No. 86 C 2363, 1986 WL 8478, at *2 (N.D. Ill. July 29, 1986) (subpoena to employers and persons who may or may not be covered by ERISA); *Shaw*, 668 F.2d at 989 (subpoena to trustee of plan arguing it was not covered by ERISA).

Here the Department merely seeks information to determine whether a fiduciary or non-fiduciary knowing participant violated ERISA; the Department is not required to show at the investigatory stage that a party is a fiduciary or violated the statute (unlike its role during an enforcement stage). *Cf. Commodity Futures Trading Comm'n v. Monex Deposit Co.*, 824 F.3d 690, 692 (7th Cir. 2016) (rejecting subpoena enforcement as forum for deciding propriety of agency's statutory determinations); *E.E.O.C. v. Sidley*

Austin Brown & Wood, 315 F.3d 696, 699-700 (7th Cir. 2002) (agreeing that EEOC may obtain facts necessary to determine whether it can proceed to enforcement).[13]

Alight's alleged non-fiduciary status does not preclude the Secretary from issuing a subpoena. Adding such a fiduciary status requirement would shield those serving plans and plan fiduciaries from any regulatory oversight unless the regulator can obtain sufficient public information about the plan or its fiduciaries. Such a reading eviscerates the Secretary's well-established role under the statute, a role which this Court could not be clearer in recognizing. "The Secretary of Labor, and only the Secretary of Labor, is authorized by Congress to represent the public interest in the enforcement of the ERISA statute." *Donovan v. Estate of Fitzsimmons*, 778 F.2d 298, 311 (7th Cir. 1985). The Secretary's "capacity to sue under ERISA advances important public interests tied to the purposes of ERISA itself, such as maintaining public confidence in funds serving thousands of employees." *Martin v. Consultants & Adm'rs, Inc.*, 966 F.2d 1078, 1089 (7th Cir. 1992). Nothing is more critical to the "public confidence" in the private benefits

[13] To the extent Alight relies on *Chamber of Commerce of the U.S. v. Hugler*, 231 F. Supp. 3d 152, 161 (N.D. Tex. 2017), Mot. at 11. *Hugler* deals with the authority to *litigate*, not to investigate.

system than the security of plan information and assets. Constraining the Secretary's ability to investigate in the way Alight proposes would threaten that public interest.

II. The District Court Correctly Held that the Subpoena is Not Too Indefinite Nor Too Burdensome

A. The Subpoena is Not Too Indefinite

The district court found that the Subpoena requests were not too indefinite, as the Secretary outlined its specific requests in 32 paragraphs and further clarified them during the litigation. R. 25 at 4. Alight asserts that the Secretary's Subpoena is too indefinite to be enforced in full, contending that this Court should reverse the district court on the grounds that the Subpoena is "sweeping," and that the district court improperly placed the burden on Alight "to establish the Subpoena *is* indefinite, rather than requiring *DOL* to establish that it is *not* indefinite." Br. at 12-14. Alight misreads the district court's opinion, which clearly states that "*the Secretary* must meet the following three requirements: (1) the Subpoena is within the authority of the agency, (2) the demand is not too indefinite, and (3) the information sought is reasonably relevant to the investigation." R. 25 at 2 (citations omitted). Once the Secretary made that showing, the burden shifted to Alight, because as another court has held, "[i]f the government

makes this preliminary showing, the burden then shifts to the respondent to prove that enforcement of the subpoena would be improper[.]" *Chao v. Koresko*, No. 04-3614, 2005 WL 2521886, at *1 (3d Cir. Oct. 12, 2005). The district court reviewed the requests, considered the Secretary's modifications, and properly concluded that "the Court cannot say that any one of them is *too* indefinite." *See* R. 25 at 4. The district court also stated that Alight's argument on indefiniteness appeared mislabeled, as it more clearly pertained to the burden of compliance, but the court clearly ruled that the Subpoena is sufficiently definite. *Id.*

Similarly, the district court properly held that Alight's argument on the "sweeping" nature of the Subpoena speaks to burdensomeness, not indefiniteness. *See id*. In *Aerotek*, the respondent claimed the EEOC requested documents "totally unrelated to the matter under investigation," and this Court concluded that respondent "makes no claim that the request is too indefinite," but rather presented the court with a question of whether the requests "impose[d] an unreasonable or undue burden." 814 F.3d at 332, 334. Alight argues the Secretary is engaged in a fishing expedition because it believes the requests are unrelated to his investigatory power. Mot. at 13-14. The district court properly classified this argument as a claim of undue burden, not indefiniteness. R. 25 at 4.

Even if this argument was about indefiniteness, it fails for two reasons: the district court found the specific requests to be sufficiently definite, *id*. at 3-4, and this Court has affirmed that an agency is not engaged in a fishing expedition when it requests specific information it regards as necessary for an investigation. *Aerotek*, 815 F.3d at 333. In *Aerotek*, the respondent argued that the EEOC improperly requested the names of more than 22,000 of its clients, including clients Aerotek had not identified as having information relevant to the inquiry. *Id*. at 332. This Court affirmed that the government has broad investigatory authority and can request information it deems necessary for its investigation, in order to assess whether anyone was violating the law it enforces. *Id.* at 333-4; *accord Commodity Futures Trading Comm'n v. Tokheim*, 153 F.3d 474, 478 (7th Cir. 1998). Similarly, the Secretary requested names of Alight's clients, which is essential to determine whether those clients violated ERISA. The Subpoena and its later modifications by the Secretary, Mot. Exhibit C, and Sec'y Opp. Exhibit B at 9-12, which specifically requests information within statutory bounds, are not indefinite, and are necessary to determine whether, for example, cybersecurity risks resulted in harm to any ERISA plans or participants. *See, e.g., United States v. Comley*, 890 F.2d 539, 542 (1st Cir. 1989); *Sec. Exch. Comm'n v. Arthur Young & Co.*, 584 F.2d 1018, 1025

(D.C. Cir. 1978); *F.T.C. v. Gibson*, 460 F.2d 605, 607 (5th Cir. 1972). "'[W]hat restrictions might be appropriate are decisions within the sound discretion of the trial court and should only be reversed for abuse of discretion.'" *Aerotek, Inc.*, 815 F.3d at 333 (citation omitted).

B. The District Court Did Not Abuse Its Discretion in Finding that Alight Failed to Prove That Its Burden Outweighed the Relevance of the Documents Sought

A "court will take steps to modify or to exclude portions of a subpoena only where the party objecting to the subpoena carries the difficult burden of showing that the demands are unduly burdensome or unreasonably broad." *F.T.C. v. Shaffner*, 626 F.2d 32, 38 (7th Cir. 1980). In order to establish error in weighing the burden of production against the relevance of the documents, Alight must establish an abuse of discretion, *McLane*, 137 S. Ct. at 1169, which "occurs only when no reasonable person could take the district court's view," *United States v. Henderson*, 337 F.3d 914, 918 (7th Cir. 2003). Alight cannot meet this standard.

Alight argues that the district court incorrectly evaluated its burden of compliance. Br. at 14-17. First, Alight misreads the findings on the balance of relevance and burdensomeness. Alight argues that even though it found the burden of compliance was "potentially significant," the court was wrong to hold the Subpoena should be enforced in its entirety on the grounds "that

burden does not outweigh the potential relevance of the requests." R. 25 at 5. Alight does not present any substantive argument that the information sought is not "reasonably relevant," and instead suggests the district court did not apply the right standard. Br. at 45-46. Alight twists language in the opinion on burden to claim that the court did not properly find that the Subpoena's requests were "reasonably relevant," only "potentially relevant."

1. Relevance

The district court considered the evidence and arguments on relevance, and held that "[c]learly records identifying specific plans as well as records of the plans themselves fall within the scope of a proper ERISA investigation." R. 25 at 4. Alight's argument disingenuously ignores the opinion's section on relevance in which the court specifically held, in a section headed "Requirement 3: The information sought must be reasonably relevant to the investigation," that the Secretary's requests as modified (R. 1-5 and Opp. Exhibit B at 10-12) "are reasonably relevant to an investigation of compliance with ERISA." R. 25 at 4-5. Alight asks this Court to overlook the district court's explicit finding of reasonable relevance, which the district court found as a prerequisite to weighing the relevance against the burden. *Id*. at 5 ("Having found that the three *Chao* requirements are met such that the Subpoena should be enforced, … the Court next considers

whether the burden on Respondent weighs against enforcement in this case… [which] requires this Court to balance the relevance of the Subpoena's requests against the burden of compliance.")

The court did not err in finding reasonable relevance, nor did the court erroneously apply the wrong standards in then weighing burdensomeness against relevance. The district court held that the information sought by the Subpoena "may be relevant to whether violations of ERISA have occurred." *Id*. Information that may be relevant to whether ERISA violations occurred, of course, are "reasonably relevant *to the investigation*," *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (emphasis added). *Id*. "An administrative subpoena will be enforced, when challenged on the basis of relevancy, if the material subpoenaed 'touches a matter under investigation[.]'" *E.E.O.C. v. Elrod*, 674 F.2d 601, 613 (7th Cir. 1982) ("mere assertion" by entity under investigation that its policy met a statutory exemption could not limit EEOC's investigation, because the assertion involved questions of fact and therefore agency needed access to relevant information upon which it could determine whether there was a violation of exemption). "The initial determination of what information is reasonably relevant is left to the investigating agency. The district court must enforce the subpoena unless the agency's determination of relevancy is 'obviously

wrong,' . . . and we must accept any determinations made by the district court that are not clearly erroneous. . . . [W]ide latitude is given to [an agency] in determining relevancy." *In re Gimbel*, 77 F.3d 593, 601 (2d Cir. 1996).

In turn, as this Court has held, a "finding by the district court that documents are reasonably relevant to a legitimate agency purpose cannot be overturned absent a showing that the factual determinations on which it is based are clearly erroneous or that the ruling itself constitutes an abuse of discretion." *Quad/Graphics*, 63 F.3d at 645. Here, the district court relied on the Declaration of Senior Investigator Loggins (Opp. Ex. A), who attested that EBSA began its investigation on discovering that "Alight processed unauthorized distributions [of plan benefits] as a result of cybersecurity breaches relating to its ERISA plan clients' accounts," "failed to disclose cybersecurity breaches and unauthorized distributions to its ERISA plan clients for months, if at all," and "repeatedly failed to restore the unauthorized distribution amounts to its ERISA plan clients' accounts." R. 25 at 2, citing R. 1-1 ¶ 3. This declaration supplied the undisputed factual basis for reasonable relevance. *See, e.g., Koresko*, 2005 WL 2521886, at *2; *Marshall v. Amalgamated Ins. Agency Servs., Inc.*, 523 F. Supp. 231, 234 (N.D. Ill. 1981) (relying on Department's affidavit). Courts consider

objections to relevance in the context of agencies' powers to investigate on suspicion that their regulations are violated before enforcement. *See, e.g., Aerotek*, 815 F.3d at 333; *Sidley Austin Brown & Wood*, 315 F.3d at 701. The relevancy requirement for an administrative subpoena is "not especially constraining." *Aerotek*, 815 F.3d at 334; *Acosta v. Shingal*, No. 5:17-mc-80119, 2018 WL 1358973, at *5 (N.D. Cal. Mar. 16, 2018) (same).

2. Burden

As to the burden of production, Alight exaggerates the Subpoena's impact, saying that it permits the Secretary to "troll through records, without respect to relevance." Mot. at 15 (citing *C.A.B. v. United Airlines, Inc.*, 542 F.2d 394, 398-99 (7th Cir. 1976); *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946)). Neither case cited by Alight support its argument that the Secretary is engaged in a burdensome fishing expedition. First, *C.A.B.* discussed the harm of permitting the Civil Aeronautics Board to have continuing general-warrant power. 542 F.2d at 395. This Court declined to hold that the agency had general-warrant powers and interpreted the Federal Aviation Act as granting "the agency access to all documents and materials *which further a valid regulatory function*." *Id*. at 401. The Secretary does not claim to have a general-warrant power, and the Subpoena is appropriately tailored to seek only records which further his valid

regulatory function of enforcing ERISA. Alight's reliance on *C.A.B.* is therefore misplaced.

Oklahoma Press also supports subpoena enforcement. In *Oklahoma Press*, the Supreme Court upheld an administrative subpoena issued under the Fair Labor Standards Act (FLSA) because "[a]ll the records sought were relevant to the authorized inquiry, the purpose of which was to determine two issues, whether the petitioners were subject to the Act, and if so, whether they were violating it." 327 U.S. at 210. The FLSA subpoena was enforced because it furthered a "lawfully authorized purpose." *Id*. at 209. Similarly, the Subpoena at issue here is enforceable because it furthers the Secretary's lawful ERISA investigation; it does not impose an unjustified burdensome request.

Finally, Alight argues that the district court miscited *Quad/Graphics*, thereby warranting reversal. Mot. at 16. Alight is correct that this Court in *Quad/Graphics* did not say "'more than 200,000 hours' (or nearly 23 years) of effort to comply was not unduly burdensome." *Id*. But neither did the district court. Instead, the district court referenced the 200,000 hours solely in the context of this Court enforcing a subpoena in *Quad/Graphics* even when "the responding party *estimated* that compliance would require more than 200,000 hours." R. 25 at 5-6 (emphasis added). The district court

recognized that Alight's general estimation of burdensomeness, like the general assertion by the company in Quad/Graphics, failed to prove an "unduly" burdensome subpoena that "would threaten the normal operation of its business." *Id.; Quad/Graphics*, 63 F.3d at 648. For example, the district court noted that the Secretary had "modified" its requests in light of Alight's objections. R. 25 at 5-6; *compare Inspector Gen., U.S. Dep't of Hous. & Urb. Dev. v. St. Nicholas Apartments*, 947 F. Supp. 386, 392 (C.D. Ill. 1996) (similarly relying on *Quad/Graphics*); *E.E.O.C. v. All. Residential Co.*, 866 F. Supp. 2d 636, 644 n.9 (W.D. Tex. 2011) (same).

Even assuming the district court miscited a factual conclusion of *Quad/Graphics,* any such mistake would be immaterial to the conclusion that Alight failed to show the Subpoena was unduly burdensome. The district court used *Quad/Graphics* as just one example of a respondent's failure to show that a subpoena was unduly burdensome. R. 25 at 4-5. Any harmless error in citing an example does not indicate a misunderstanding of the law or an abuse of discretion.[14]

[14] This Court acknowledged that "[a]n error that would not (if corrected in time) have altered the judge's conclusion is a harmless error, and therefore not a ground for reversal." *Kwasny v. United States*, 823 F.2d 194, 196 (7th Cir. 1987).

Aside from *Quad/Graphics*, the district court rested largely on *United Air Lines, Inc.*, a case in which this Court found that "the presumption is that compliance [with an administrative subpoena] should be enforced" and the subpoena respondent "carries the difficult burden of showing that the demands are unduly burdensome." 287 F.3d at 653. *United Air Lines* also explained that to assess burdensomeness, the court must "weigh the likely relevance of the requested material to the investigation against the burden to [the respondent] of producing the material." *Id*. (quoting *E.E.O.C. v. Ford Motor Credit Co.*, 26 F.3d 44, 47 (6th Cir. 1994)). The district court followed this balancing test and ruled that the relevance of the requests to the Department's investigation outweighs the time Alight might need to expend to comply. R. 25 at 5-6. The district court cited *Quad/Graphics* to illustrate the point that a subpoena is not unduly burdensome just because of the respondent's assertion that compliance requires many hours of work. *Id*. The district court's use of *Quad/Graphics* does not change its ruling in favor of the Secretary under the *United Air Lines* balancing test.

Regardless, the district court undoubtedly did not abuse its discretion. Multiple circuits, including this Court, when weighing the burden against relevance in the balancing test, look at the burden of compliance holistically to evaluate whether the hours or cost of responding to the subpoena would

"seriously and unreasonably disrupt [respondent's] business." *S.E.C. v. Savage*, 513 F.2d 188, 189 (7th Cir. 1975); *accord E.E.O.C. v. Ranstad*, 685 F.3d 433, 451 (4th Cir. 2012) (evaluating undue burden "in light of the company's normal operating costs"); *United States v. Chevron USA, Inc.*, 186 F.3d 644, 649 (5th Cir. 1999) (holding a subpoena was not unduly burdensome because Chevron did not explain how, given its size, the cost and effort of compliance would threaten its normal business operations); *F.T.C. v. Texaco*, 555 F.2d 862, 882 (D.C. Cir. 1977). As such, a district court's analysis of undue burden "depends on the particular facts of each case and no hard and fast rule can be applied to resolve the question." *United Air Lines*, 287 F.3d at 653 (quoting *Shaffner*, 626 F.2d 38). Under this test, in *E.E.O.C. v. Groupon, Inc.*, the Northern District of Illinois found that an administrative subpoena was not unduly burdensome, even though the respondent estimated that compliance "would require three to five temporary staff and five to ten hours per week from one permanent employee" for about four months. 16-C-5419, 2016 WL 5110509, at *5 (N.D. Ill. Sept. 21, 2016). The district court in *Groupon* compared the hours needed to respond to the subpoena against the company's resources, which included over 1,900 employees in the Chicago office alone. *Id*. Groupon, as a large company with ample resources, could not prove that the subpoena

was unduly burdensome simply because it required thousands of hours of work. *Id*. Similarly, Alight, which purports to have about 15,000 employees,[15] has not explained why compliance constitutes an undue burden that would threaten its normal business operations.

This Court has recognized that "any subpoena places a burden on the person to whom it is directed." *Shaffner*, 626 F.2d at 37. The district court properly articulated that courts will not strike down burdensome subpoenas; they will only intervene in instances where the responding party shows that the subpoena is *unduly* burdensome. R. 25 at 5 (quoting *United Air Lines*, 287 F.3d at 653). Courts have found that even large requests are not necessarily *unduly* burdensome, as in *Groupon* where the EEOC requested documents related to "at least 25,000 applications over the relevant time period." 2016 WL 5110509, at *5. The Ninth Circuit held that an administrative subpoena was not unduly burdensome even though the respondent claimed that it would require them to request over one million documents from another company. *F.D.I.C. v. Garner*, 126 F.3d 1138, 1145-46 (9th Cir. 1997). The Tenth Circuit acknowledged that an

[15] Alight's website states that it has 15,000 employees who serve at least 4,000 clients in over 100 countries. Alight (Feb. 2, 2022, 6:08 PM ET), https://alight.com/about. *See also* Mot. at 3-4 (noting that it is a "global" business supporting 20.3 million participants).

administrative subpoena may be "inconvenient and involve some expense" when respondent submitted an affidavit estimating it would "require two full-time employees working approximately six months," but nevertheless held that this was not unduly burdensome. *E.E.O.C. v. Citicorp Diners Club, Inc.*, 985 F.2d 1036, 1040 (10th Cir. 1993). Courts have held that the "mere fact that compliance with the subpoenas may require the production of thousands of documents is … insufficient to establish burdensomeness" because the "mere size of the [subpoenaed company's] operation is no excuse for its refusal to give information." *N.L.R.B. v. Carolina Food Processors*, 81 F.3d 507, 513 (4th Cir. 1996) (citing *N.L.R.B. v. G.H.R. Energy Corp*, 707 F.2d 110, 114 (5th Cir. 1982) and *N.L.R.B. v. United Aircraft Corp.*, 200 F. Supp. 48, 51 (D. Conn. 1961), *aff'd*, 300 F.2d 442 (2d Cir. 1962). In short, courts have held that subpoenas can be inconvenient and require significant amounts of work without rising to the level of being unduly burdensome. Alight has pointed to an obvious fact that compliance will require work, but has not demonstrated why it expects that its compliance obligation passes the high threshold of being *unduly* burdensome.

Apart from the fact that Alight has not shown the requested production will threaten its normal course of business, Alight has not

provided sufficient evidence to support its estimations of the time it would take them to comply. "Conclusory allegations of burdensomeness are insufficient" to illustrate an undue burden. *United Air Lines*, 287 F.3d at 653 (citing *Shaffner*, 626 F.2d at 38). It is not enough for parties to simply say that compliance with the subpoena would be disruptive; this Court has looked to whether the respondent has also provided estimates of the "number of files involved, the number of estimated work hours required to effect compliance, [or] the estimated costs of compliance." *Shaffner*, 626 F.2d at 38. Even when a respondent provides estimates, this Court has still enforced the subpoena when the estimates are inflated, as in *Quad/Graphics*. First, Alight offers no estimates of the number of documents it will need to recover to comply with the Subpoena, nor do they provide the court with estimates of the cost of compliance. Rather, Alight relies on one declaration detailing the time it took one individual to produce documents that they said showed a two-month sample of incidents. Br. at 48-49. Based on this one declaration, Alight makes the conclusory statement that compliance will require a vague "thousands of hours of work." *Id*. It is unclear if this number is inflated, and this conclusory claim provides neither the Secretary nor this Court with a clear understanding of Alight's outstanding burden of compliance.

Second, even if the Court accepts the unsupported claim of "thousands of hours" as an estimate, the district court as fact finder did not find that this was unduly burdensome so as to outweigh the relevance of the documents. Marsha Dodson's declaration, offered by Alight, explains that she spent over 40 hours retrieving two months' worth of documents. R. 15-1 at ¶ 19. Counsel for Alight, in her declaration, states that Alight produced 240 documents in total, for March 2018 and January 2019 investigative summaries. R. 15-2 at ¶¶ 31, 37. In total, these documents are only 562 pages. *Id*. Alight does not explain why it took over 40 hours to retrieve such a small batch of documents, nor does it clarify why this two-month sample is representative of every month for which the Secretary seeks documents, e.g., whether the months sampled may have been unusually busy ones. Alight did not provide the district court with adequate information to address any of these questions and simply failed to provide the district court with the information necessary to show undue burden. It was Alight's burden of proof to provide sufficient evidence of showing that compliance would be, not just a burden, but unduly burdensome such that it would seriously hinder normal business operations. Instead, Alight offered vague, potentially inflated estimates without concrete evidence, and the district

court weighed the facts and found that it failed to meet its exceedingly high burden of showing that such burden was undue.

This Court should also take note of the fact that Alight created some of its purported burden unnecessarily by redacting the vast majority of documents, rendering them useless to the investigation by making it almost impossible to ascertain what documents are related to each other and which documents relate to which client. Opp. at Exhibit C, 9-10. Alight cannot undertake burdens not required by the Subpoena or the court and then use them to thwart a Subpoena. *See Aerotek*, 815 F.3d at 333-34 (affirming enforcement of subpoena where company increased the burden on itself by creating coding system to mask identity of individuals and clients in earlier non-compliant productions, and where the court notes that the agency's investigation involving company's clients "obviously would be ineffectual if [company] refuses to reveal the names of its clients."). The district court properly ruled in favor of the Secretary because Alight did not prove that the Subpoena is unduly burdensome.

III. The District Court Correctly Denied Alight's Request for a Protective Order.

In order to obtain a protective order, the district court "must independently determine if 'good cause' exists" to enter the protective order.

Jepson, Inc. v. Makita Elec. Works, Ltd., 30 F.3d 854, 858 (7th Cir. 1994). The moving party has the burden to show good cause. *Id.* If good cause is not shown, then the materials are not entitled to "judicial protection." *Id.* "To show good cause for a protective order, the moving party is required to make 'a particular and specific demonstration of fact, as distinguished from stereotyped and conclusory statements.'" *In re Nat'l Prescription Opiate Litig.*, 927 F.3d 919, 929 (6th Cir. 2019); *In re Terra Int'l, Inc.*, 134 F.3d 302, 306 (5th Cir. 1998).

The district court's decision is reviewed for an "abuse of discretion." *Phillips ex rel. Ests. of Byrd v. Gen. Motors Corp*., 307 F.3d 1206, 1210 (9th Cir. 2002); *In re Nat'l Prescription Opiate Litig.*, 927 F.3d at 929.

Alight claims that the district court incorrectly denied its request for a protective order, but provides no explanation of how this constitutes an abuse of discretion. Br. at 49-50. Alight argues that three categories of information must be protected: "(1) ERISA plan participant [personally identifiable information (PII)]; (2) confidential settlement agreements; and (3) client identifying information." *Id.* at 50.

A. Participant PII

Alight claims, based on a hypothetical situation in which a third-party may obtain allegedly confidential documents from the Secretary, that

producing documents to the Secretary would lead to "[t]he disclosure of these details about how illicit third parties targeted plan participants, in conjunction with the names of the plan participants [which] would expose these plan participants and cases, their spouses and families to significant harm and potential embarrassment by exposing to the world not only their financial information, but also their personal information and their possible susceptibility to third-party cybersecurity threats." Br. at 51-52. First, Alight assumes without basis that such information would be disclosed to a third party when the disclosure is to the government. As stated to Alight, and confirmed by the district court, confidential information is protected from disclosure under FOIA. R. 25 at 6-7; 5 U.S.C. §§ 552(b)(4) and (6) (FOIA exemptions protect confidential business information and PII from disclosure); 29 C.F.R. § 70.26 (providing submitter the opportunity to prevent disclosure of its information under FOIA); *see generally U. S. Dep't of State v. Wash. Post Co.*, 456 U.S. 595, 601 (1982). Furthermore, there is no current FOIA request, so any risk is completely speculative. *Solis v. Food Emps. Labor Rels. Ass'n*, 644 F.3d 221, 230 (4th Cir. 2011) ("Contrary to the Funds' contention, the potential for public disclosure in the investigation context does not harm beneficiary interests any more than in the enforcement context. And, while the potential for disclosure under a

Freedom of Information Act request may be somewhat burdensome, the Secretary has cited several available exceptions which make the likelihood of disclosure pursuant to such a request remote."); *cf. Aerotek*, 815 F.3d at 334 (affirming enforcement of subpoena where company objected that production would harm business relationships, but provided no basis for this speculation); *Dole v. Milonas*, 889 F.2d 885, 889 (9th Cir. 1989) (rejecting "generalized speculation"). As this Court noted in *F.T.C. v. MacArthur*, 532 F.2d 1135, 1143 (7th Cir. 1976), "[s]anctions are provided in Section 10 of the Federal Trade Commission Act (which imposes a maximum fine of $5,000, maximum imprisonment of one year, or both) for unauthorized disclosure of information obtained by the Commission (15 U.S.C. § 50)," undercuts the need for a protective order. *See* 29 U.S.C. § 1134(c) (applying 15 U.S.C. § 50 to investigations under ERISA).

As shown by these cases, Alight's suggestions that PII is not protected in disclosures to the government is unsupported by cases involving parties that are not the federal government. *See* Br. at 52-53. In fact, the cases Alight cited favor the Department's position. For example, in *Martinez v. City of Chi.*, No. 09-cv-5938, 2012 WL 1655953 at *2 (N.D. Ill. May 10, 2012), the district court noted that FOIA protections (state protections in that case) are consulted in understanding "good cause," specifically whether

privacy interests are implicated. *Id.* In that case, the district court noted that a court could even *reject* a protective order that accords with FOIA protections, because a party had not established good cause for such equivalent protections. *Id.* at *3; *accord Henry v. Centeno*, No. 10 C 6364, 2011 WL 3796749, at *6 (N.D. Ill. Aug. 23, 2011). Here, any disclosure to the Secretary will be accorded full protection afforded by FOIA and DOL regulations.

B. Confidential Settlement Agreements

Alight argues that "DOL also seeks confidential settlement agreements that Alight entered into with clients related to potential unauthorized access and disbursements to client accounts. . . . Barring the disclosure of Alight's settlement agreements, which contain information with minimal, if any, relevance to DOL's purported investigation, would protect the confidentiality of the parties' settlements and thus support the judiciary's long-standing policy of protecting those materials from disclosure and use as a means of encouraging settlements." Br. at 53 (citing Fed. R. Evid. 408).

Alight makes a basic error in conflating admissibility under the Federal Rules of Evidence and disclosure during discovery. "Information within this scope of discovery need not be admissible in evidence to be

discoverable." Fed. R. Civ. P. 26(b)(1); *see, e.g., Parrott v. United States*, 536 F.3d 629, 638 (7th Cir. 2008) ("the district court relied (inappropriately) on rules of admissibility and generalized concerns about privacy and confidentiality, rather than on the basis of discoverability."). Alight's general arguments would shield all settlements with confidentiality clauses from discovery. Br. at 53-54 (making general policy arguments).

Confidentiality clauses *cannot* shield agreements from discovery categorically, and Alight cites no cases to the contrary. *See, e.g., DIRECTV, Inc. v. Puccinelli*, 224 F.R.D. 677, 685 (D. Kan. 2004) ("Simply put, litigants may not shield otherwise discoverable information from disclosure to others merely by agreeing to maintain its confidentiality."); *Cooley v. Curves Int'l, Inc.*, No. A-08-MC-108 LY, 2008 WL 11333881, at *4 (W.D. Tex. May 19, 2008) ("Courts routinely order production of confidential settlement agreements under Rule 26 when they are relevant to the allegations at issue in a particular action."). "Indeed, as one district court noted, "[a]mong the federal courts, there is a general consensus that confidential settlement agreements are discoverable." *TIGI Linea Corp. v. Pro. Prod. Grp.*, LLC, No. 419CV00840RWSKPJ, 2021 WL 1947341, at *7 (E.D. Tex. May 14, 2021) (noting that courts dismiss arguments based on

Federal Rule of Evidence 408 and confidentiality clauses) (citing authorities).

In fact, courts have highlighted the role of the Secretary in examining ERISA settlements to determine if such settlement serves plan participant and public interests. *E.g., Fitzsimmons*, 805 F.2d at 695 (en banc) (concerning a settlement agreement that shielded information from the DOL); *Herman v. S.C. Nat. Bank*, 140 F.3d 1413, 1426 (11th Cir. 1998). Preventing regulators from subpoenaing settlements because of their confidentiality clauses shields these settlements from the Secretary's statutory role to protect plan participants and the public interest.

C. Client-identifying Information

Finally, Alight argues that "DOL's Subpoena seeks broad categories of client information including contracts and fee schedules, information related to investigations of alleged cybersecurity and fraud, documents concerning services and security measures applicable to a given plan, and other proprietary information about Alight's client's benefit plans." Br. at 54-56. This information is critical for DOL to assess whether Alight and fiduciaries operating its client benefit plans are abiding by ERISA duties to protect *plan* participants and the public interest. *See, e.g., Fitzsimmons*, 805 F.2d at 692-93; *Food Emps. Labor Rels. Ass'n*, 644 F.3d at 232. Indeed,

what Alight terms "client" information is more accurately described as "ERISA plan" information. Viewed in this way, DOL's interest in obtaining this data is obvious, as Alight's "actual" clients are the plan participants. *Food Emps. Labor Rels. Ass'n*, 644 F.3d at 232 (agreeing with "several courts [that] have found that the [fiduciary] exception [to attorney-client privilege] similarly applies to the work product doctrine, reasoning that a trustee's attorney should not withhold work product from the actual client, i.e. the trust beneficiaries."). Redacting the "client," *i.e.*, "plan," name as suggested, Br. at 55-56, would not permit the Secretary to identify and protect the interests of the "actual client," the plan participants and beneficiaries. Without identification of the "plan" the Secretary cannot determine *who* may have violated ERISA. 29 U.S.C. § 1134(a).

Plan information is key to an ERISA investigation because the Secretary needs to know *who* is implicated, including which fiduciary. While Alight makes an argument based on its *contractual* commitments, those contracts cannot protect the agreements from being disclosed to the Secretary in an ERISA investigation, because ERISA states that "any provision in an agreement or instrument which purports to relieve a fiduciary from responsibility or liability for any responsibility, obligation, or duty under this part shall be void as against public policy." 29 U.S.C. § 1110. If

confidentiality provisions in settlements could protect them from being disclosed in an agency investigation, they would be insulating fiduciaries from liability in violation of ERISA. "While Alight's contracts vary from client-to-client, every contract contains a 'Confidential Information' provision that designates, as confidential: (a) the terms of the agreement (including Schedules and other attachments to the Agreement); (b) Client Information; (c) oral and written information designated by a party as confidential prior to the other party obtaining access thereto; and (d) oral and written information that should reasonably be expected to be treated as confidential by the recipient whether or not such information is designated as confidential. (*Id.*)." R. 30, at 3. Alight cannot negotiate with clients to shield clients and incidents from regulatory scrutiny.

D. Relevance of Each of The Preceding Categories

Alight also recycles its arguments that its clients' confidential information is not relevant in its request for a protective order. *Id*. But the district court already ruled that the documents requested are relevant to EBSA's investigation. Confidential information will help the Department identify any harm to specific participants, assess harms, and identify witnesses to potential breaches or violations. And the district court found that "Respondent has not shown why the Secretary, who is bound by law to

protect confidential information, should not be entitled to receive records beyond those containing de-identified data." R. 25 at 6. Alight does not explain why it believes the district court erred on either of these determinations; it simply disagrees. Mere disagreement with the district court's evaluation is not grounds for reversal on appeal. *See Dow Chem. Co. v. Allen*, 672 F.2d 1262, 1278 (7th Cir. 1982) (upholding decision without much justification); *Mejia v. Pfister*, 988 F.3d 415, 419 (7th Cir. 2021) (holding a disagreement with a decision is not an abuse of discretion).

In any event, each category of information referenced by Alight is relevant to ERISA enforcement goals. First, ERISA plan "information including contracts and fee schedules" provide important information as to whether arrangements with service providers are reasonable. *E.g., Solis v. Current Dev. Corp.*, 557 F.3d 772, 779 (7th Cir. 2009) ("The statute requires that the services be pursuant to a contract or a reasonable arrangement, that they are necessary for the plan's operation, and that they cost no more than what's reasonable.") (citing 29 U.S.C. § 1108(b)(2)). Second, as noted earlier, cybersecurity is an important regulatory concern here and a significant aspect of the plan and its service provider's duties to uphold ERISA fiduciary obligations. So, "information related to investigations of alleged cybersecurity and fraud, documents concerning services and security

measures applicable to a given plan, and other proprietary information about Alight's client's benefit plans" directly assist in ascertaining whether those duties are upheld. Ultimately, Alight cannot hide behind its agreements with clients to shield the plans from regulatory scrutiny that serves to protect plan participants and the public interest. *E.g., Fitzsimmons*, 805 F.2d at 695. Alight, with potential liability as a knowing participant in a breach or as a functional fiduciary, has a conflict of interest in preventing access to information. *See Beck v. Levering*, 947 F.2d 639, 642 (2d Cir. 1991) (noting that the Secretary may need to protect plans when trustees or fiduciaries "faced with potential lability and their interest in absolving themselves" would not act); *see also* 29 U.S.C. § 1110; *cf. IT Corp. v. Gen. Am. Life Ins. Co.*, 107 F.3d 1415, 1419 (9th Cir. 1997) (noting that the participants did not sign any agreement to shield the fiduciaries from liability).

CONCLUSION

The Secretary requests this Court affirm the district court's order to enforce the Secretary's Subpoena.

Respectfully submitted,

Date: February 18, 2022

SEEMA NANDA
Solicitor of Labor

G. WILLIAM SCOTT
Associate Solicitor for
Plan Benefits Security

THOMAS TSO
Counsel for Appellate
and Special Litigation

/s/ Robin Springberg Parry
ROBIN SPRINGBERG PARRY
Senior Regulatory Attorney
Plan Benefits Security Division
Office of the Solicitor
U.S. Department of Labor
200 Constitution Ave. NW
Room N-4611
Washington, DC 20210
(202) 693-5600

RACHEL UEMOTO
Trial Attorney

CERTIFICATE OF COMPLIANCE

I hereby certify that:

1. This brief conforms to type-volume limitations provided in Fed. R. App. P. 3(a)(7) because it contains 12,741 words.

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and Seventh Circuit Rule 32(b), and the type-style requirements of Fed. R. App. P. 32(a)(6), because it was prepared using Microsoft Word 2016 and is written in 14-point, proportionately spaced Times New Roman font.

/s/ Robin Springberg Parry

Attorney for U.S. Department of Labor
Office of the Solicitor
Plan Benefits Security Division

Dated: February 18, 2022

CERTIFICATE OF SERVICE

I hereby certify that on the 18th day of February, 2022, I electronically filed the foregoing with the Clerk of the Court of the United States Court of Appeals for the Seventh Circuit by using the CM/ECF system. I certify that all participants in this case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: February 18, 2022 /s/ Robin Springberg Parry