The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 34367

November 17, 2022

DOL Responds to Joint Trade Letter That Expressed Serious Concerns with DOL Collection of Personally Identifiable Information

[34367]

November 16, 2022

TO: ICI Members
Pension Committee
Pension Operations Advisory Committee
Privacy Issues Working Group SUBJECTS: Pension
Privacy RE: DOL Responds to Joint Trade Letter That Expressed Serious Concerns with DOL Collection of Personally Identifiable Information

In September, ICI and several other trade organizations[1] submitted the attached letter to the Department of Labor (DOL) expressing concern regarding DOL's use of subpoena power to collect vast amounts of retirement plan participants' confidential, personally identifiable information (PII). DOL responded with a letter (attached), affirming its intention to continue collecting PII as part of its cybersecurity investigations.

Joint Trade Letter to DOL

While our concern is not limited to one particular case, the issue was brought to our attention because of a subpoena DOL issued to Alight Solutions LLC (a non-fiduciary service provider, providing recordkeeping services to plans), to examine its cybersecurity practices. The subpoena sought to obtain extensive disclosures, including plan participants' confidential information and PII, including names, home addresses, phone numbers, email addresses, social security numbers, banking information, asset information, investment information, beneficiary information, and contribution levels. After Alight contested the subpoena (after attempts to resolve the issue by providing a redacted version of documents), DOL petitioned the district court to enforce the subpoena, and won, both in district court and the Seventh Circuit Court of Appeals.[2]

The joint trade letter, addressed to Secretary of Labor Marty Walsh, did not dispute DOL's right to request relevant information in connection with its investigations. Instead, it suggested a collaborative effort to determine how best to help participants and plan

sponsors without creating unnecessary risks for them. It expressed our concern that by demanding the release of large amounts of unredacted plan-related information, including PII, DOL is creating substantial risk regarding participant data security. In light of the reality that every transmission of PII creates new risks,[3] the letter suggested that DOL should use redacted information to make an assessment of whether a breach occurred. Then, if necessary, the relevant confidential information could be released upon finding a breach.

The letter urged DOL to incorporate four basic principles with respect to its information security practices:

- Recognize security risks and safeguard data on hand.
- Collect only necessary data, request redacted or anonymized participant data until a breach is confirmed and promptly destroy data and information once it is no longer needed.
- Report and notify the public of any breach that occurs.
- Limit access to any information collected by DOL to only those at DOL assigned to the investigation.

DOL Response to Letter

In November, DOL's Employee Benefits Security Administration (EBSA) responded to the letter, largely rejecting the concerns raised by the joint trades and affirming its intention to continue collecting PII in its cybersecurity investigations.

DOL's letter makes the following assertions:

- "[G]iven the large cyber security breaches that have occurred over the past few years, cyber criminals likely already have many participants' [PII]," in effect, suggesting that the sole focus should be on service providers' controls to prevent unauthorized access, rather than on prevention of disclosure and protection of the PII.
- EBSA is careful to request the data it needs to complete its investigations, and PII is critical to resolving factual issues, pursuing leads, and resolving the scope and nature of ERISA violations.
- EBSA has systems and protocols in place to prevent the loss of PII and protect all data during use, transit, and storage. Further, EBSA employees and contractors are regularly trained on cybersecurity threats and protection.

The letter further noted DOL's cybersecurity guidance for plan sponsors, plan fiduciaries, record-keepers and plan participants issued in 2021.[4]

Shannon Salinas
Associate General Counsel - Retirement Policy

Notes

[1] In addition to ICI, the signatories include: U.S. Chamber of Commerce, The SPARK Institute, Small Business Council of America, SIFMA, National Association of Professional Employer Organizations, National Association of Insurance and Financial Advisors, Insured Retirement Institute, The ERISA Industry Committee, and American Benefits Council.

[2] Walsh v. Alight Solutions LLC, No. 21-3290 (7th Cir. Feb. 18, 2022). See Walsh v. Alight Solutions, LLC, No. 20-cv-02138, U.S. District Court for N. District of Illinois, October 28, 2021, affirmed, No. 21-3290, U.S. Court of Appeals for the Seventh Circuit, August 12, 2022. Among other arguments, Alight argued that a protective order is needed to prevent disclosure of certain confidential information. The Seventh Circuit did not find this argument persuasive.

While this information is sensitive, Alight has not shown how its disclosure to the Department would result in the information being revealed to a third party. As the district court observed, this confidential information is protected from disclosure under the Freedom of Information Act, and 18 U.S.C. § 1905 criminalizes the disclosure of confidential information by federal employees. Alight's only attempt to show good cause for the protective order is to note that the Department has experienced some data breaches and cyberattacks in the past.

See page 17 of the Seventh Circuit's opinion, available at www.govinfo.gov/content/pkg/USCOURTS-ca7-21-03290/pdf/USCOURTS-ca7-21-03290-0.pdf.

[3] The letter noted that numerous government systems have previously been compromised and that DOL's own Office of Inspector General has expressed its concern about DOL's ability to safeguard its data and information systems.

[4] For an overview of the guidance, see ICI Memorandum No. 33475, dated April 16, 2021, available at https://www.ici.org/memo33475.
