M | M | P | L

EMPLOYEE BENEFITS LAW

Seventh Circuit Confirms DOL's Authority to Investigate Plan Service Provider's Cybersecurity

In Spring 2021, the DOL issued guidance to plans, recordkeepers, and participants on cybersecurity best practices to safeguard plan assets and personal information. Since then, the DOL has begun auditing plans' cybersecurity practices and requesting documents such as cybersecurity policies, proof of service provider practices, and information on past breaches. A recent Court of Appeals case out of the Seventh Circuit, *Walsh v. Alight Solutions LLC*, confirms the DOL's broad authority.

The case stems from the DOL's investigation into Alight Solutions, a large third-party plan recordkeeper. Alight allegedly experienced cyberbreaches that resulted in improper distributions of plan benefits. Upon learning of the distributions, the DOL issued a subpoena to Alight, asking for Alight's client list, contracts, fee schedules, and security protocols. After pushback from Alight, the DOL sought and the district court granted its petition to enforce the subpoena. On appeal, Alight argued the DOL lacked the authority to investigate non-fiduciaries such as Alight, and cyber breaches generally. Alight also challenged the scope of the subpoena and claimed it should be permitted to redact client-identifying information.

The Court of Appeals rejected all of Alight's arguments:

- It confirmed the DOL can investigate a non-fiduciary so long as there's a connection to an alleged ERISA violation.
- It concluded Alight didn't timely raise its argument on the DOL's authority to investigate cybersecurity matters, but in dicta said the DOL's investigations into cybersecurity practices are relevant to determine violations of ERISA's duties of loyalty and care.
- It cautioned that its decision should not read as carte blanche for agencies to make overly cumbersome or irrelevant requests.
- It decided that Alight could not redact its client and plan names because the DOL needed to be able to identify which plan may have violated ERISA.

The case is a good reminder that the DOL is actively investigating cybersecurity deficiencies and has broad investigative powers. Even if a plan itself isn't the initial target of an investigation, a service provider's security failures could lead to an investigation of the employer and plan.

Per the DOL's Spring 2021 guidance, MMPL recommends that plan fiduciaries arrange to (1) document that service providers' cybersecurity practices have been evaluated, (2) establish a cybersecurity policy, (3) include cybersecurity terms in its service providers' contracts, and (4) purchase cybersecurity insurance.