CYBERSECURITY ENFORCEMENT RISKS FOR ERISA PLAN SPONSORS

Employers that sponsor ERISA retirement or health plans should anticipate the Department of Labor taking a more aggressive enforcement stance in regard to the cybersecurity of those plans.

ERISA is enforced by DOL's Employee Benefits Security Administration ("EBSA"). Recently, EBSA published new cybersecurity guidance for plan sponsors, plan fiduciaries, record-keepers, and plan participants (available at: https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414). With over $9.3 trillion in ERISA retirement plans, plan fiduciaries have an obligation to take appropriate precautions to mitigate the risks of internal and external cybersecurity threats.

EBSA's guidance has three components:

- Online Security Tips - a page-and-a-half document aimed at plan members and beneficiaries, which employers may find advisable to circulate to their members and beneficiaries (available at: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf).
- Cybersecurity Program Best Practices – aimed at recordkeepers and other service providers responsible for plan-related IT systems and data, this five-page document sets forth a 12-element set of best practices that plan sponsors should look for when choosing a service provider (available at: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf).
- Tips for Hiring a Service Provider with Strong Cybersecurity Practices – aimed at plan sponsors, this two-page document provides a list of questions that sponsors should ask when contracting with and monitoring service providers. Those questions are designed to test the service provider's compliance with the Cybersecurity Program Best Practices. This sponsor-focused document also suggests specific terms to include in service provider contracts to enhance the cybersecurity of the sponsor's plan (available at: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf).

Of note, EBSA's website lists "failing to properly select and monitor service providers" as an ERISA violation subject to civil enforcement by DOL.

Plan sponsors should take particular note of the guidance regarding contracts with service providers. Such contracts should "ensure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches."

EBSA also suggests the following contract provisions:

- Information Security Reporting. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.
- Clear Provisions on the Use and Sharing of Information and Confidentiality. The contract should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.
- Notification of Cybersecurity Breaches. The contract should identify how quickly the plan sponsor would be notified of any cyber incident or data breach. In addition, the contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.
- Compliance with Records Retention and Destruction, Privacy and Information Security Laws. The contract should specify the service provider's obligations to meet all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information.
- Insurance. A plan sponsor may want to require insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage.

This cybersecurity guidance was published on EBSA's website, and does not have the force of an official "rule." As such, failing to comply with the guidance and its "best practices" may not, alone, subject an employer to an enforcement action. However, EBSA also notes that the guidance "compliments EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries. These include provisions on ensuring that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems include measures calculated to protect Personally Identifiable Information." As such, the guidance should be read as clarification of cybersecurity obligations that already have the force of regulation. In other words, plan sponsors would ignore this guidance at their peril.

For more information about cybersecurity planning, policies and best practices, please contact PLDO Principal William E. O'Gara and Partner Joel K. Goloskie at 401-824-5100 or email wogara@pldolaw.com and jgoloskie@pldolaw.com.

Joel K. Goloskie
Partner

William E. O'Gara
Principal

PANNONE LOPES DEVEREAUX & O'GARA LLC
counselors at law