LEGAL UPDATE

The DOL's New Cybersecurity Audits and Informal Guidance

Marcia S. Wagner, Esq.

Recently, the Department of Labor (DOL) has become highly focused on the cybersecurity practices of plan sponsors and their service providers. Perhaps in response to the growing number of ERISA cyber breach cases, the Employee Benefits Security Administration of the DOL issued cybersecurity guidance on April 14, 2021. In its guidance, which is directed toward plan participants, service providers, and plan sponsors, the DOL addresses ways to minimize cyber breaches and thefts from participants' accounts, as well as cyber fraud and the misappropriation of confidential participant information, and warns plan fiduciaries about prudent selection and ongoing monitoring of service providers that have access to participant information and assets.

Current DOL Audits

The DOL had begun asking cybersecurity questions on some plan audits in 2020, but recently began using a more comprehensive document request in plan audits. The DOL's cybersecurity document request to plan sponsors is broadly stated: "all documents relating to any cybersecurity or information security programs that apply to the data of the plan, whether these programs are applied by the sponsor of the plan or by any service provider to the plan." The audit request asks for, among other things:

- policies, procedures, or guidelines related to the sponsor's cybersecurity practices;

- past cybersecurity incidents;
- risk assessment and security control audit reports;
- security reviews, system development programs, and technical controls; and
- documents and communications regarding service provider cybersecurity capabilities, policies, and procedures.

The DOL has indicated informally that the purpose of the audit inquiries is information gathering, rather than enforcement, and the type of situation that would trigger enforcement activity by the DOL against a plan sponsor would likely be an inadequate response to a breach of which the plan sponsor was notified. Nevertheless, it is important for plan sponsors to know and understand what cybersecurity issues are, act in a manner that reduces and minimizes the risk of a cyber breach, and verify that its service providers also are taking appropriate steps.

The DOL does not mandate that plan sponsors adopt a formal cybersecurity policy outlining the sponsor's policies and procedures, the same way it does not mandate adopting an investment policy statement outlining its investment guidelines, but it clearly regards such conduct as a fiduciary best practice. The DOL further indicates that a plan's cybersecurity policy should be the predicate for requiring a service provider to have a similar or better cybersecurity policy.

The Wagner Law Group has prepared cybersecurity policies for adoption by plan sponsors. The policy reflects the DOL's April cybersecurity guidance as well as certain elements of the privacy and security policies of the Department of Health and Human Services for group health plans with respect to HIPAA. Adopting a comprehensive cybersecurity policy such as ours is one way a plan sponsor can show it takes cybersecurity seriously.

Marcia S. Wagner *is the Managing Director of The Wagner Law Group. She can be reached at 617-357-5200 or* Marcia@WagnerLawGroup.com.