



DOL Issues Cybersecurity Guidance for Plan Fiduciaries

Chad DeGroot
05.21.2021

In April, the U.S. Department of Labor (DOL), for the first time, issued cybersecurity guidance that was focused on retirement plans governed by the Employee Retirement Income Security Act of 1974 (ERISA) but could be applicable to many different benefit plans subject to ERISA. The guidance, which was provided by the DOL's Employee Benefits Security Administration (EBSA) in the form of tips and best practices, does not have the impact of law or formal regulations, but it does set forth the DOL's expectations and recommendations as to plan sponsors and fiduciaries with respect to protecting against and mitigating cybersecurity risks. The guidance sets forth specific tips for:

1. hiring service providers to maintain plan records and keep participant data confidentiality
2. recordkeepers and service providers to manage cybersecurity risks, and
3. online security for plan participants and beneficiaries.

However, a general takeaway for plan sponsors and other plan fiduciaries may be that it is now clear that the DOL takes the position that fiduciaries have an obligation to manage and guard against cybersecurity risks and that this may become a focus of DOL investigations in the near future. As a result, and considering the guidance provided, now would be an opportune time for plan sponsors and other fiduciaries to adopt cybersecurity policies that align with the DOL recommendations and consider purchasing cyber

Practice Areas

Counseling and
Transactional

Employee Benefits and
Executive Compensation

Retirement Plans



DOL Issues Cybersecurity Guidance for Plan Fiduciaries

liability insurance to protect against breaches of cybersecurity.