LEGALcurrents®

April 19, 2021

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

EMPLOYEE BENEFITS AND EXECUTIVE COMPENSATION
PRIVACY AND DATA SECURITY

DEPARTMENT OF LABOR ISSUES CYBERSECURITY RECOMMENDATIONS FOR BENEFIT PLANS

On April 14, 2021, the U.S. Department of Labor issued new cybersecurity recommendations for benefit plans governed by the Employee Retirement Income Security Act of 1974, as amended ("ERISA"). The guidance, available at https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity, covers data security, anti-fraud and business continuity/disaster recovery concerns, and consists of a list of topics for retirement plan fiduciaries to discuss with potential vendors, an outline of cybersecurity best practices for plan vendors, and a list of recommendations for plan participants seeking to keep their account information secure. While the guidance assumes that fiduciaries will be outsourcing plan recordkeeping, it reinforces the idea that securing sensitive information is a fiduciary responsibility generally. Accordingly, similar principles and considerations should be taken into account with respect to employer in-house systems.

Plan fiduciaries and their IT advisors should review the Department's recommendations with their vendors. They should confirm that existing plan and vendor practices and systems are in line with the Department's expectations, or document the reasons why any aspects of the guidelines are not appropriate in their circumstances. Periodically, fiduciaries should revisit their security protocols and vendor relationships to be sure that their protocols and their vendors' operations and contract terms remain in line with best practices in this evolving area. In addition, fiduciaries should be sure they receive appropriate reporting on plan data security audits conducted by the plan sponsor and plan vendors. In the event of reported defects or security incident reports, fiduciaries should make sure that appropriate remedial action is taken. Finally, plan fiduciaries should ensure that cybersecurity issues are properly addressed for future vendor relationships and when contracts for existing vendors are renewed, and should update any internal checklists and procurement protocols used for these processes as needed.

Separately, fiduciaries should take advantage of opportunities to remind participants to take appropriate precautions for their plan accounts. A link to the Department's recommendations may be a convenient resource to include in participant communications on that topic.

Although the DOL's recent recommendations are provided in the form of "best practices" and useful "tips," it is important to note that a growing number of states throughout the country have enacted laws that *require* similar cybersecurity safeguards to be implemented by any entity operating within their borders or otherwise holding the data of their residents, including mandated vendor management procedures, data-related risk assessments and written security programs. The extent to which ERISA preempts these laws

Practice Group Leader
Paul W. Holloway

Health and Welfare
Thomas J. Hurley
John W. Brill

Counsel
Leslie E. DesMarteau
Lisa G. Pelta
Joseph E. Simpson

Associates
Amanda M. Karpovich

Benefits Litigation
Jessica N. Clemente
Erika N. D. Stanat

Retirement
Mark R. Wilson

Executive Compensation
Christopher M. Potash

remains unsettled. Therefore, employers and vendors should be mindful of these rules, and should consult counsel with any questions about their applicability to specific situations and relationships. Likewise, employers and plan fiduciaries should bear in mind that health plans are subject to specific requirements under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and other laws.

If you have any questions regarding this LEGALcurrents, please contact any member of the Employee Benefits and Executive Compensation or Privacy and Data Security groups at 585.232.6500 or 716.853.1616, or visit www.hselaw.com.