FYI®
For Your Information®

Volume 44

Issue 20

May 25, 2021

Authors
Mary H. Roth, JD, MLT
Fred Farkash, CEBS, Fellow-ISCEBS
Melissa Maher, CEBS

DOL issues cybersecurity guidance for retirement plan sponsors and fiduciaries

While cybercrime was already on the rise prior to 2020, its acceleration during the pandemic has illuminated the financial risks associated with lax cybersecurity protocols. On April 14, DOL waded into the fray with its first guidance on fiduciary responsibilities for the online security of participant benefits and information.

Background

In February 2021, the Government Accountability Office (GAO) issued a report recognizing the significant cybersecurity risk to personal information and assets in employer-sponsored defined contribution plans and estimating the total assets at risk at approximately $6.3 trillion as of 2018. GAO urged the DOL to clarify whether plan administrators are responsible for mitigating cybersecurity risks under ERISA and set expectations for protecting the personal information of employer sponsored defined contribution plans. GAO's report only mentioned the risk to defined contribution plans, but its rationale is broader and can easily be applied to other retirement and welfare plans subject to ERISA.

Best practices and tips

DOL responded to GAO's recommendation by issuing two documents to assist retirement plan sponsors, plan administrators and plan service providers.

This guidance makes it clear that DOL views the mitigation of cybersecurity risks as a plan fiduciary obligation that cannot be avoided by assigning responsibility for data security to a third party. Failure to act prudently can expose a plan fiduciary to liability from DOL and private litigants.

The first document lists and describes twelve Cybersecurity Program Best Practices and clarifies that "responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks." The guidance is specifically directed to recordkeepers and other service providers responsible for plan-related IT systems, and to plan fiduciaries charged with prudently selecting and monitoring plan service providers.

The best practices include (but are not limited to): having a formal, well-documented cybersecurity program, conducting annual risk assessments and third-party audits of security controls, limiting user access to data based on a "need to know" standard with access reviewed at least quarterly, conducting cybersecurity awareness training at least annually, applying data encryption standards to protect data at rest and in transit, requiring third-party vendors (including cloud providers) to follow similar protocols, and responding appropriately to cybersecurity incidents and breaches.

The second document provides Tips for Hiring a Service Provider with Strong Cybersecurity Practices to guide plan fiduciaries in engaging recordkeepers and other third parties who maintain plan records and participant data. The contracting tips, like the best practices, are detailed and comprehensive.

The DOL also provided Online Security Tips for participants that plan administrators are encouraged to disseminate.

DOL did not specify, as they did in their recent best practices for missing participants, that plan administrators should consider the facts and circumstances in deciding what steps are appropriate. The comprehensiveness and specificity of these rules create the real possibility that they will be used by DOL as a baseline for determining fiduciary breaches and by plaintiffs seeking to sue plan fiduciaries for alleged breaches.

Recent litigation highlighting cybersecurity risks in retirement plans.

The Barnett vs. Abbott Labs, et. al., case demonstrates what is at risk with cybertheft of plan assets. In this case the ERISA claim against the plan sponsor was dismissed but moves forward against the recordkeeper.

In closing

Cybersecurity is a growing societal concern, and plan sponsors and fiduciaries should take the guidance issued by the DOL as a sign that they are taking these issues more seriously for retirement plans. These rules are a significant step toward bringing retirement plan data security up to the level that HIPAA demands of covered entities (and business associates) under group health plans. Furthermore, the DOL guidance may come to be regarded as a minimum level of compliance by the DOL and plaintiffs. Plan sponsors and fiduciaries should review the best practices and contracting tips and consider using them as a guide for the selection and monitoring of administrative service providers (internal and external) and other plan vendors and reviewing their contract terms with plan

service providers. Additionally, plans sponsors should consider distributing the participant online security tips to raise cybersecurity awareness and help them protect themselves.

COVID-19 Compliance check-in

Buck's latest version of the **COVID-19 Compliance check-in** is updated to reflect the retirement, health, labor and employment issues facing employers now. Review the checklist to help your team manage priorities and determine next steps.

Produced by the Compliance Consulting Practice

The Compliance Consulting Practice is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, training, and knowledge management. For more information, please contact your account executive.