DOL urged to give retirement plans cybersecurity guidance

By Geoff Manville and Brian J. Kearney
April 7, 2021

Citing reports of cybersecurity breaches and stolen funds from retirement accounts, a recent Government Accountability Office (GAO) report urges the Department of Labor (DOL) to issue guidance to help defined contribution (DC) plans guard against these threats. In the report to leaders of House and Senate committees that oversee ERISA, GAO recommends DOL formally state that plan fiduciaries are legally responsible for mitigating cybersecurity risks. GAO also calls on DOL to issue cybersecurity guidance detailing specific steps for plans to protect participant accounts and personally identifiable information (PII).

Guidance coming

DOL officials told GAO that they believe cybersecurity is a serious problem for retirement plans, and the department plans to post subregulatory compliance assistance materials addressing related issues for plan sponsors and administrators. But the timing of DOL's coming cybersecurity guidance is uncertain. GAO's report did not recommend legislation, but lawmakers will likely assess the need for action after reviewing the DOL guidance.

Regarding cybersecurity as a fiduciary responsibility under ERISA, DOL officials suggested that this is already implicitly required under ERISA's broad fiduciary standards and existing electronic notice and disclosure rules. DOL believes that ERISA's fiduciary obligations require managing cybersecurity risks to retirement plan assets and PII. For example, retirement plan sponsors should ask questions about cybersecurity measures when retaining service providers and periodically monitor the provider's compliance with those procedures.

Prior calls for guidance. Cybersecurity issues are not new to DOL, which has conducted investigations and prosecutions related to cybersecurity incidents over the years. In addition, DOL's ERISA Advisory Council has recommended — most recently in 2016 — guidance on how sponsors should evaluate and manage cybersecurity risks to plan data and participants' personal information — especially risks involving third-party relationships for plan administration.

Patchwork of rules

The GAO report notes that even though the retirement industry has a broad array of tools and information to help sponsors address cyber risks, these standards are generally voluntary. Federal law imposes some protections, but they generally apply only to certain service providers, leaving out others that work with sensitive information. For

example, financial institutions are subject to federal legislative and regulatory requirements to safeguard the privacy of consumer data, but those rules may not apply to plan sponsors that aren't financial institutions or to plan service providers that handle only administrative functions.

"As a result, plan fiduciaries and their service providers rely on a patchwork of federal regulations, guidance, and industry leading practices to … mitigate cybersecurity risk in DC plans," lawmakers said in response to the GAO report. "Until DOL formally clarifies plan fiduciaries' responsibilities and provides minimum expectations related to cybersecurity, fiduciaries may not realize that they could be liable for losses they were obligated to prevent, and plans and their participants will continue to be vulnerable to financial losses and PII breaches."

Liability for breaches unclear

According to the report, a major source of vulnerability comes from the data that plan sponsors and administrators share electronically, including participants' Social Security numbers, addresses and birth dates. In some cases, the report noted, individuals employed by the plan sponsor made unauthorized withdrawals from participants' accounts.

Attorneys cited in the report said that who bears the risk for losses from these security breaches is sometimes ill-defined and left to the courts to sort out. Although ERISA fiduciaries can be held personally liable for breaches, DOL officials noted that fiduciaries might not be able to cover the losses due to the large amount of money at risk in retirement accounts. Cyber insurance may enable plan sponsors and service providers to recover some costs caused by an attack. But those policies often have caps on payouts, exclude certain types of attacks or don't cover funds stolen from participants' accounts.

Related resource

- Federal guidance could help mitigate cybersecurity risks in 401(k) and other retirement plans (GAO, March 15, 2021)

Note: Mercer is not engaged in the practice of law, accounting or medicine. Any commentary in this article does not constitute and is not a substitute for legal, tax or medical advice. Readers of this article should consult a legal, tax or medical expert for advice on those matters.