GROOM LAW GROUP

Investigations & Enforcement

Developing a Prudent Process for Cybersecurity

ATTORNEYS & PROFESSIONALS

Allison Itami
aitami@groom.com
202-861-0159

Kevin L. Walsh
kwalsh@groom.com
202-861-6645

PUBLISHED
08/26/2021

SOURCE
PLANSPONSOR

SERVICES
Audits & Investigations

As the Department of Labor (DOL) expands the Swiss Army knife of skills it expects a retirement plan fiduciary to have, it becomes more important than ever for fiduciaries to focus on having verifiable processes in place.

We've previously said that having a verifiable administrative process can be helpful when the DOL investigates. In recent years, we have been helping plan fiduciaries who have been focused on developing bounty-hunter-like policies in response to the agency's aggressive enforcement position on missing participants. As the DOL pivots to new areas of enforcement—such as cybersecurity—it will be important for plan fiduciaries to consider taking similar steps to help protect participant account balances, plan information technology systems and related information. While nobody could have anticipated in 1974 (when the Employee Retirement Income Security Act [ERISA] was enacted) that plan fiduciaries would be responsible for cybersecurity, here we are in 2021 with a department that seems to expect human resources (HR) professionals to moonlight as expert hackers.

In the *PLANSPONSOR* article, "Developing a Prudent Process for Cybersecurity," Groom principals Allison Itami and Kevin Walsh outline steps for plan sponsors to take to both prepare for and avoid DOL cybersecurity audits, especially as the Department has prioritized cybersecurity investigations.

To read the article, click here.