Bloomberg Law News 2021-10-05T09:08:55836-04:00

Small U.S. Retirement Plans Lagging in Cybersecurity Oversight

By Austin R. Ramsey 2021-10-05T05:30:48000-04:00

- Recordkeepers can influence fiduciary roles
- DOL enforcement audits already underway

Many small U.S. retirement plan sponsors aren't evaluating the tech firms they've hired to protect user data even with recent U.S. Labor Department guidance and stepped-up enforcement.

A Cerulli Associates Inc. quarterly report late last month found that while the majority of plan advisers consider cyber health an important part of choosing a recordkeeper, most small-to-mid-sized plans still don't have formal written processes for overseeing their recordkeepers' fraud prevention practices.

As the DOL ups its cybersecurity enforcement and litigation emerges, plan fiduciaries become solely responsible for sensitive information about their participants falling into the wrong hands under someone else's watch.

"The plan fiduciaries are the ones who have the ultimate responsibility to mitigate risk," said Jeanne Klinefelter Wilson, a principal attorney at Groom Law Group Ctd., who headed the DOL's Employee Benefits Security Administration under former President Donald Trump. "It's up to them when they hire someone to keep records and to consider a lot of factors, including cybersecurity."

Fiduciaries at large, sophisticated plans tend to understand that responsibility and have resources and staff to regularly assess contractors' fraud and data controls, Wilson said. Smaller firms can be left in the dark. As recordkeepers themselves continue to make cyber improvements, they may play an outsized role in helping their smaller clients keep up, she added.

"One of the things they need to be doing is helping raise awareness to plan fiduciaries that they have this responsibility," Wilson said. "Most recordkeepers have very robust systems in place; they've been doing it all along."

‘Tidal Wave Is Coming’

EBSA issued its first-ever guidance on retirement cybersecurity in April, part of what it characterized as an ongoing effort to establish best practices in the industry and protect workers’ benefits from a growing online threat.

The agency’s Cybersecurity Program Best Practices and Tips for Hiring a Service Provider partly focus on the third-party service providers such as recordkeepers or administrators that plan sponsors hire to help them manage retirement plans.

But EBSA’s jurisdiction only extends to fiduciaries who have discretionary authority or control over plan assets. Plan sponsors who may lack the training or experience needed to vet another company’s cyber practices are still legally bound to do so.

Often, DOL will use its regulatory control over fiduciaries to shift industry behavior, but the Cerulli report found that recordkeepers responsible for tracking and managing retirement assets already have systems in place. Instead, small-plan fiduciaries meant to exert pressure brought on by federal regulators aren’t holding up their end of the bargain.

Great-West Lifeco Inc.-owned Empower is one of the nation’s largest and fastest-growing recordkeeping firms, and it takes the data its clients entrust very seriously, Keith Mancini, Empower Retirement assistant vice president of government affairs, said at an Insured Retirement Institute conference last week. But most of its smaller plan sponsors haven’t yet caught on to the DOL’s new cybersecurity focus, and they may pay a compliance cost.

“I think the tidal wave is coming,” said Mancini.

Enforcement and Exclusion

In the months after EBSA issued its cybersecurity guidance, it became clear the agency’s subregulatory nudge had morphed into an enforcement priority. Questions about cybersecurity documentation, detailed processes, and fiduciary insurance have been tacked onto ongoing audits, benefits attorneys have said. While those efforts don’t seem punitive, they’re costly and time

consuming.

For those smaller plans that do understand their newly redefined fiduciary responsibilities, their size may exclude them exercising it, said Sarah Bassler Millar, a partner at Faegre Drinker Biddle & Reath LLP in Chicago.

“To what extent can smaller or mid-sized employers effectively monitor vendors when the vendors are so big?” she said. “These plans have a lot less negotiating power with big recordkeepers, so how can they effectively fulfill their fiduciary responsibilities when, for example, contract language may not be negotiable?”

It may not matter that recordkeepers are ramping up their cybersecurity practices if smaller employers who are responsible for their participants’ data and information can’t access the information they need to document it. That’s why Millar said she tells her clients to prioritize that documentation, highlighting the need for proof in their requests for information and in regular communications with their vendors.

“I think, at a minimum, it’s important to ask the questions,” she said. “We’ve seen this story play out in other areas in the past; when lots of different employers are asking the same questions, it moves the needle for these big recordkeeping firms.”

To contact the reporter on this story: Austin R. Ramsey in Washington at aramsey@bloombergindustry.com

To contact the editor responsible for this story: Martha Mueller Neff at mmuellerneff@bloomberglaw.com

Related Articles

Asset Manager Mergers Can Warrant Fresh Looks From Plan Sponsors

Retirement Plan Cybersecurity Audits Shock Unprepared Industry

Employee Benefits Agency Issues First Cybersecurity Guidance (1)

Punching In: White House Mulling Order on Contract Labor Pacts

Related Documents

Tips for Hiring a Service Provider

Cybersecurity Program Best Practices