Retirement News Highlights

Friday, August 18, 2023

MOVEit cyberattack ignites worry about fiduciary responsibility

By Margarida Correia
Pensions & Investments
August 17, 2023

If there's one big takeaway for plan sponsors following the massive MOVEit cyberattack that breached the personal data of millions of participants in public pension and private-sector workplace retirement plans, it's this: They may need to rewrite their vendor contracts and redouble their monitoring of service providers.

While no sponsors have yet been sued, it's not far-fetched to think that they could be, according to legal experts.

"I'm just waiting for a court to start looking at what did the plan sponsor do in order to determine whether there were adequate safeguards in place," said Carol Buckmann, founding partner at Cohen & Buckmann PC in New York.

Plan sponsors could also be audited by the Department of Labor, though it's more likely that their vendors will come under scrutiny instead, said a top Department of Labor official.

In situations like the latest MOVEit hack, the DOL's Employee Benefits Security Administration "often would look at the service provider and understand what they were doing," said Ali Khawar, EBSA's principal deputy assistant secretary, in an interview.

However, plan sponsors would not be entirely off the hook.

"There may be plan-level investigations that flow from that," Mr. Khawar said, referring to potential vendor audits. "There may be individual plans where we're kind of looking at it to better understand what's happening to all of the plan clients."

The cyber thieves, identified as Russian ransomware gang Clop, attacked thousands of organizations globally — not just companies serving pension and retirement plans — by exploiting vulnerabilities in the MOVEit file transfer application used by Pension Benefit Information LLC and other vendors to securely transfer encrypted files.

PBI is widely used by retirement plan record keepers and others in the industry to provide end-to-end encryption services and conduct death audits to identify deceased participants. The company declined to comment beyond a statement on its website saying it was among many other entities impacted by the cyberattack.

To date, the breach impacted public pensions systems in at least 10 states, including the $465.7 billion California Public Employees' Retirement System, Sacramento, and the $309.3 billion California State

Teachers' Retirement System, West Sacramento, affecting almost 1.2 million participants and beneficiaries; retirement plans in Tennessee, Rhode Island, Virginia and others. Several record keepers were also affected by the hack, including Fidelity Investments, Teachers Insurance and Annuity Association of America, and Corebridge Financial, formerly AIG Life & Retirement.

So far, at least 3.8 million participants in public pension and private-sector retirement plans are known to have been affected.

The breach at Fidelity via its vendor PBI leaked data on more than 370,000 participants in Fidelity record-kept retirement plans, according to a notification on the website of Maine's attorney general office.

A spokesman for Fidelity confirmed that a "limited number of plan sponsors" had been affected and emphasized that Fidelity's systems had not been breached.

"We are not aware of any identity theft issues and continue to monitor the situation," the spokesman said in an email.

Corebridge Financial also confirmed that one of its vendors, which it did not disclose, had been affected by the MOVEit file transfer vulnerability.

The record keeper declined to say how many plan sponsors and participants were affected.

"We are actively working with the vendor to investigate the scope and nature of customer data that was impacted. This is being done in coordination with leading forensic investigators engaged by the vendor," a notice on Corebridge's website said.

TIAA also confirmed that it had been impacted through its vendor PBI but declined to disclose the number of plan sponsors that were hit. The Maine notification, however, reported that more than 2.3 million TIAA customers were affected.

TIAA was sued in federal court in New York by a former teacher claiming the firm failed to protect her personal data in the cyberattack.

"We are in contact with impacted institutional clients. Through PBI, any affected individuals will be offered free credit monitoring for two years at no cost to them," a TIAA spokesperson said in an email.

TD Ameritrade Holding Corp., now owned by Charles Schwab Corp., was also hurt by the MOVEit breach, although less than 0.5% of its brokerage clients had their data leaked, according to a Schwab spokeswoman. None of Schwab's retirement plans were affected, she said.

Top 10 breach

While the full scale and severity of the breach have yet to be determined, many observers characterize it as significant — but not materially worse — than other breaches involving personally identifiable information.

Jay Gepfert, managing partner at cyber assessment firm DOL Cybersecurity LLC in Norwalk, Conn., sees the breach as being in the top 10 because the number of people affected crossed the significant 1 million mark.

"That's like a billion-dollar lottery ticket," he said, alluding to the fact that most people only pay attention to the lottery when it reaches $1 billion.

Regulators are paying attention.

The DOL's Mr. Khawar says the agency has expectations of plan sponsors and their vendors as spelled out in guidance it released in 2021.

The DOL is interested in finding out what questions plan sponsors were asking their service providers and what process they went through to hire them, Mr. Khawar said.

"To the extent they weren't evaluating the cybersecurity posture of a service provider when they were making that hiring decision, that would be something I think we would be concerned about," he said.

Even though the breach occurred at the subcontractor level, in this case PBI and the MOVEit file transfer provider Progress Software, some lawyers believe that plan sponsors could be liable.

Legal experts argue that the DOL made clear in its guidance in 2021 that it is the plan sponsor's fiduciary duty to assess its service providers.

"To the extent that vendors have personal data or have access to the accounts that maintain that data for participants or beneficiaries in the plans, you have to have an understanding of what their cybersecurity is," said Joseph Lazzarotti, a principal in the Berkeley Heights, N.J., office of Jackson Lewis PC.

Mr. Lazzarotti said that the layers of vendor relationships make it difficult to assess how far plan sponsors need to go to vet the vendors they choose. If the sponsor selects a record keeper that then hires another vendor to subcontract some of the work, "where does the plan sponsor's duty end?" he asked.

"It's an interesting question. I don't know where the answer lies, but it does raise questions," Mr. Lazzarotti said.

For Ms. Buckmann, there's little doubt in her mind that plan sponsors can be liable, even if the breach occurred deep down in the vendor chain.

If it's an ERISA plan, sponsors can be sued on the grounds that they breached their fiduciary responsibilities in not properly monitoring service providers and investigating their practices before they were hired, Ms. Buckmann said.

"It's not a slam-dunk win," she said. "It may be an uphill battle in court, but I think there's a basis in the law for taking that position and trying to litigate it."

To mitigate a plan sponsor's risk of getting sued, Ms. Buckmann includes a provision in all service contracts that she negotiates for plan sponsors with vendors. The provision says that while the vendor is free to use subcontractors, it is responsible for the work of that subcontractor as if it were part of the vendor's workforce.

As made explicit in the provision, subcontractors are considered direct employees, which means that the service provider's indemnification obligations for negligence apply to the work that's done by subcontractors too, Ms. Buckmann said.

Some legal experts, however, don't think plan sponsors should be concerned about being legally liable for a hack that no one could have expected.

David Levine, principal at Groom Law Group in Washington, argued that because PBI is a well-known, widely used business in the retirement industry, it's hard to attribute blame to plan sponsors, which he said are already vigilant and asking lots of security questions as part of the contracting process.

"I would expect as part of the different levels of diligence that their vendors do matching market practice, I think it's hard to say that they're liable," Mr. Levine said. "It's a hard argument to make."

Mr. Levine's thinking echoes Mr. Khawar's general views about the cyberattack.

"It doesn't follow from my perspective that a cybersecurity breach means that there was absolutely a fiduciary violation," Mr. Khawar said, adding that there is "no such thing as a foolproof system."

Nevertheless, in Mr. Khawar's view, there are two possible scenarios that need to be weighed when assessing plan sponsor liability.

A plan sponsor that did everything it could to prevent breaches from happening is very different from the plan sponsor or vendor that "casually emails," say, a notepad document filled will Social Security numbers instead of sending it through a secure file transfer system.

"That's not really the same thing as an entity that has all their data encrypted," Mr. Khawar said.

Back to top