LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Unclear Cyber Guidance May Lead To ERISA Case Spike

By **Joshua Gmerek** (September 27, 2021, 2:22 PM EDT)

Joshua Gmerek

Lack of clarity surrounding the causation standard under Section 409(a) of the Employee Retirement Income Security Act could lead to more litigation as cyberattacks on retirement plans increase.

In April of this year, the U.S. Department of Labor issued cybersecurity guidance directed toward retirement plan sponsors, plan fiduciaries, record-keepers and participants. While not necessarily groundbreaking, this long overdue guidance lays out what the government believes are some best practices for record-keepers and plan fiduciaries when it comes to a retirement plan's cybersecurity.

These best practices include practices like using multifactor authentication and encryption of sensitive data stored and in transit. Maybe unexpectedly, however, this guidance has the potential to impact ERISA litigation through the causation standard set forth in Section 409(a) of ERISA.

ERISA Section 409(a) provides that a plan fiduciary who breaches his/her fiduciary duties is personally liable for losses to the plan resulting from his/her breach. While determining whether a loss results from a breach is not difficult for many types of ERISA claims, that determination might not be as easy in lawsuits involving lost assets due to cyberattacks.

For example, in an ERISA action claiming excessive fees were paid by the plan, it is not hard to draw the line of causation directly from the fiduciary's insufficient plan administration and oversight process to the loss sustained by the plan — i.e., paying excessive fees. With a claim stemming from a cybersecurity breach, however, it can be harder to draw this direct line.

If a cybercriminal gets a hold of an individual's online retirement account password through no fault of a fiduciary, there is no Section 409(a) claim. But what if multifactor authentication would have prevented this unauthorized distribution and the plan did not have it in place? In light of the DOL's subregulatory guidance earlier this year directed at plans governed by ERISA, does failing to incorporate a recommended security feature establish sufficient causation for a Section 409(a) claim?

It should be briefly noted that this guidance does not affirmatively state whether failing to mitigate cybersecurity risks is a breach of fiduciary duty. However, it is clear that the DOL believes that fiduciaries should be taking some steps to mitigate these cyber risks otherwise they would not have issued this guidance.

As it stands now, it is unclear what level of causation is required to have a viable claim under Section 409(a) as circuit courts have been relatively silent on the issue. This is potentially due to the fact that causation often is not disputed during ERISA lawsuits.

Regardless, the U.S. Court of Appeals for the Eleventh Circuit holds that proximate cause is the standard in an ERISA case.[1] This would require a showing that the harm alleged has a sufficiently close connection to the conduct — or lack thereof — at issue.

In contrast, the U.S. Court of Appeals for the Second Circuit has merely noted in passing that some causal link between the breach and the loss is required.[2] This vague language leaves much to be desired, and it is likely the Second Circuit will not adopt this broad of a standard, but until they elaborate more, everyone is left in the dark.

It is possible the Second Circuit agrees that proximate cause is the standard and they are just waiting for the issue to be presented to them before formally stating so. It is equally possible that the Second Circuit could find that one of the other numerous causation standards is appropriate — e.g., but for, substantial nexus, etc. — so this issue is far from settled.

To my knowledge no court has looked at the causation component of an ERISA Section 409(a) claim stemming from a cyberattack. Outside of the ERISA context, however, courts have looked at similar questions.

In 2014, hackers were able to retrieve sensitive personal information from over 20 million former and present government employees by breaching multiple U.S. Office of Personnel Management databases. In a lawsuit stemming from that hack, the U.S. Court of Appeals for the D.C. Circuit in In Re: U.S. Office of Personnel Management Data Security Breach Litigation found in 2019 that proximate cause was sufficiently alleged when a complaint contended that the OPM's failure to establish information security safeguards consistent with industry standards was the proximate cause of the stolen personal information.[3]

While this case did not deal with benefit plans, it suggests a court might be willing to look at industry practices in the causation analysis at the pleading stage which could be relevant to a future ERISA claim. Does the DOL subregulatory guidance discussed above establish industry-standard safeguards for ERISA plans? If the DOL has its way, it likely would.

Education — of both plan fiduciaries and plan participants — is a huge part of being able to competently protect against cyberattacks and the DOL subregulatory guidance makes this clear. The saying "a chain is only as strong as its weakest link" captures the essence of why education is so important here.

Plan fiduciaries can adopt and implement all the best practices recommended by the DOL, but if a single plan participant is tricked, that may be all that is needed for an attack. According to a report published earlier this year by the Government Accountability Office, the most common types of cyberattacks on retirement plans come in the form of malware, ransomware, phishing and spoofing among others.[4]

In 2021, everyone should take some time to understand how these attacks are carried out. This knowledge is important not just for ERISA plan purposes, but for daily life in general at this point.

Unfortunately, a number of individuals have already had their retirement accounts attacked, but I am

not aware of any major successful cyberattacks on a retirement plan as a whole. Hopefully it stays this way, but plan fiduciaries cannot assume it will.

Thus, plan fiduciaries should move to the top of their to-do list the implementation of the practices identified in the DOL's guidance along with any other security measures that may protect their plan. Don't be the case that answers the questions posed in this article.

Joshua Gmerek is an associate at Hodgson Russ LLP.

[1] Willett v. Blue Cross & Blue Shield of Alabama, 953 F.2d 1335, 1343–44 (11th Cir. 1992).

[2] Silverman v. Mut. Ben. Life Ins. Co., 138 F.3d 98, 104 (2d Cir. 1998).

[3] In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 67 (D.C. Cir. 2019).

[4] U.S. Government of Accountability Office, GAO-21-25, Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans (2021). https://www.gao.gov/assets/gao-21-25.pdf.