

# CAUSATION UNDER ERISA IN A CYBERSECURITY WORLD

*Hodgson Russ Employee Benefits Newsletter*  
September 8, 2021

The causation standard under Section 409(a) of ERISA is an issue that could lead to more litigation as cyberattacks on employee benefit plans increase. 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 when a loss results from a breach is often not that difficult for many ERISA claims, as more lawsuits involve lost assets due to cyberattacks, this has the potential to change.

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 administration process to the loss sustained by the plan (i.e. paying excessive fees). With a claim stemming from cybersecurity, however, it is harder to draw this direct line. If a cybercriminal gets ahold of an individual's online retirement account password through no fault of a fiduciary, the individual has no 409(a) claim. But what if multi-factor authentication would have prevented this unauthorized distribution and the plan didn't have it in place? In light of the Department of Labor's guidance earlier this year directed at retirement plans, does failing to incorporate a recommended security feature provide sufficient connection for a 409(a) claim?

As it stands now, it is unclear what level of causation is required to have a viable 409(a) claim. This is potentially due to the fact that causation often isn't a large focus of dispute during ERISA claims. The Eleventh Circuit holds that proximate cause is the standard. 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 Second Circuit has merely noted that "some causal link" between the breach and the loss is required. This vague language leaves much to be desired because, in some sense, everything has some causal connection. Of course the Second Circuit won't adopt this broad of a standard, but until they elaborate more, everyone is left in the dark.

To my knowledge, no court has looked at the causation component of an ERISA 409(a) claim stemming from a cyberattack. Outside of the ERISA context, however, courts have looked at similar questions. Back in 2014, hackers were able to retrieve sensitive personal information from over twenty-million former and present

## Attorneys

Peter Bradley  
Michael Flanagan  
Richard Kaiser  
Ryan Murphy  
Amy Walters

## Practices & Industries

Employee Benefits

## CAUSATION UNDER ERISA IN A CYBERSECURITY WORLD

government employees by breaching multiple U.S. Office of Personnel Management databases. In a lawsuit stemming from that hack, one circuit court found that proximate cause was sufficiently alleged when a complaint contended that the defendant's failure to establish industry-standard information security safeguards was the proximate cause of the stolen personal information. While this case did not deal with benefit plans, it shows that at least one court is willing to look at industry practices in the causation analysis at the pleading stage which could be relevant to an ERISA claim.

