

Blog Post

Does Traditional ERISA Fiduciary Liability Insurance Adequately Protect Retirement Plan Sponsors from COVID-Related Cyber Liability? Not Always

April 21, 2020

By [Beth Alcalde](#) and [Christy S. Hawkins](#)

Employer-sponsored retirement plans have long been targets for cybercriminals. The COVID-19 pandemic has expanded the types and likelihood of potential cyber attacks against retirement plan accounts. After all, with many more Americans working remotely, interfacing with the secure plan recordkeeping sites is occurring around the clock from a wide range of personal computing devices. Americans have more reason now than ever to stay on top of their retirement accounts, due to a combination of general market uncertainty, workforce disruptions, and the adoption of corporate 401k plan amendments pulling back on company matching contributions or revising the definition of plan-eligible compensation definition. Also, the CARES Act relaxed plan in-service distribution rules in the event of a COVID financial strain, and similarly expanded 401k plan loan procedures for COVID reasons. (See [our analysis of the CARES Act's employee benefits provisions](#)) It is arguable that never before have plan participants been flocking to this extent to their retirement plan accounts and remotely initiating various elective directions to plan custodians.

Related People

[Beth Alcalde](#)
[Christy S. Hawkins](#)

Related Work

[Employee Benefits and Executive Compensation Tax](#)

Related Offices

[Dallas](#)
[West Palm Beach](#)

Coronavirus Resource Center

[Visit the Resource Center](#)



This new reality has set the stage for emerging areas of cyber liability. There are a number of helpful tips for employers sponsoring retirement plans in times of pandemic. For example, many plan sponsors are working with their outside plan recordkeepers to develop enhanced substantiation of electronic transfer instructions. From a fiduciary oversight perspective, plan fiduciaries are also taking seriously their obligations to review and monitor over time the privacy and security systems of their outside plan service providers. Also, plan fiduciaries are reviewing their existing ERISA fiduciary liability insurance policies, cyberinsurance, fidelity bonds, and general corporate errors and omissions policies to ascertain whether COVID-related cyber liability is already covered, or rather if a separate endorsement is available and advisable. Specifically, policies or endorsements should cover a variety of fact patterns involving business email compromise scams such as the following:

- when a bad actor obtains the credentials for an company's existing employee who is authorized to interact with a retirement plan service provider, and then postures as that employee in order to send fraudulent wire instructions to a plan trustee or custodian to misdirect contributions to or distributions from the retirement plan;
- when a bad actor obtains the credentials for one of the company's retirement-plan service providers and sends improper instructions to that plan sponsor with fraudulent wire instructions, instructing the corporate plan sponsor to pay the bad actor instead of the real outside vendor; or
- a combination of the above.

In many instances, separate insurance endorsements will be needed. Proceeding without adequate insurance is risky, given that the ultimate question of which entity(ies) would bear responsibility for plan losses is critical but unsettled. These types of compromise scams present a

relatively new issue, and the law is far from settled across the U.S. In fact, in many jurisdictions, this issue has not even been addressed by published court opinions. Therefore, companies that sponsor qualified retirement plans should work with their insurance brokers and outside privacy and security advisers to evaluate and mitigate such risks.

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.