

Keeping Plan Data Safe: Cybersecurity in Retirement Plans

Washington is considering steps necessary to protect retirement plans from cyberattacks.

By David Levine, Diana McDonald, and Brigen Winters

It's every recordkeeper's — and plan sponsor's — nightmare: a data breach. In the 21st century, as the amount of personal data held by companies across the country seemingly grows by the minute, how are we as a society ensuring that data's safety?

That's the question the Senate Commerce Committee — not one that those of us in the retirement world usually focus on — sought to answer on February 27 during a hearing entitled, "Policy Principles for a Federal Data Privacy Framework in the United States." The hearing aimed to shed light on data privacy in the U.S. and what actions Congress could take to create protections for all Americans. As Senator Roger Wicker (R-MS), the Committee Chairman, said in his opening remarks, "In an age of rapid innovation in technology, consumers need transparency in how their data is collected and used. It is this committee's responsibility and obligation to develop a federal privacy standard to protect consumers without stifling innovation, investment, or competition." While the hearing didn't come up with a solution, the lawmakers and the witnesses all agreed that a bipartisan solution providing clear rules is not just a necessity, but an imperative.

In the narrower retirement context, Senator Patty Murray (D-WA), Ranking Member of the Senate HELP Committee, and Representative Bobby

Scott (D-VA), Chairman of the House Committee on Education and Labor, sent a letter earlier in February to the Government Accountability Office ("GAO") asking them to study cybersecurity in the private retirement system in the U.S. The letter asks the GAO to examine current procedures in place and weigh whether existing legal requirements are sufficient to protect plan participants. The letter also asks the GAO to consider whether requiring a cybersecurity bond in addition to the existing ERISA fiduciary bond would be appropriate or helpful.

The letter to the GAO acknowledges that digital interactions are increasingly common and important in retirement savings — and that retirement plans are tempting targets for cybersecurity attacks due to the wealth of information and assets they hold. The letter states that although there are industry efforts to strengthen collective cybersecurity and facilitate information sharing, cybersecurity safeguards, risks and liabilities are ill-defined for plan sponsors and participants. This is due to the patchwork of federal and state laws on the subject — and nothing in ERISA specifically addresses the numerous cybersecurity questions.


The letter identifies ten areas for the GAO to address, including:

- identifying facts including what potential threats cyberattacks present to retirement well-being,

- the preparedness of sponsors and providers,
- whether existing federal agency policies deter potential cyberattacks involving retirement savings, and
- existing legal requirements at the state and federal level and internationally.

Further, the request asks the GAO to address what protections should exist in this area including:

- what steps should plan sponsors be required to take,
- should cybersecurity insurance be mandatory,
- should there be a federal cybersecurity insurer, and
- ultimately, what legislative or regulatory steps could bolster the protection of data and the retirement accounts.

This issue has been percolating for a number of years now. In its 2016 report, DOL's ERISA Advisory Council asked the DOL to provide guidance for plan sponsors in this area, but to date no guidance has been released. 

David Levine is a Principal at Groom Law Group, Chartered.

Diana McDonald is a Senior Policy Advisor at Groom Law Group, Chartered.

Brigen Winters is a Principal at Groom Law Group, Chartered.