VOL. 34, NO. 2 SUMMER 2021

BENEFITS LAW JOURNAL

From the Editor

It's All Geek to Me: DOL Fights Cybercrime

Tech-savvy crooks can pilfer a pension or 401(k) plan from thousands of miles away. As huge depositories of money and valuable personal information, retirement plans are likely targets. Yet, many plan sponsors and benefits professionals have assumed that cybercrime was primarily someone else's responsibility – the IT department, recordkeepers, mutual fund companies, etc. Well, not quite. Chastised by the Congressional Budget Office for not "clarifying" fiduciaries' responsibility for mitigating cybercrime risks and protecting plan assets, the U.S. Department of Labor ("DOL") released a tryptic of sensible how-to cyber security advice: one for employers/sponsors, another for service providers and a third for participants.

I admit it took me several reads through the DOL guidance, released on April 14, to understand that the DOL has done an admirable job with a task outside its comfort zone. And, as I confirmed with some plan recordkeepers and the family geek, the recommended actions are both sensible and already widely adopted. Importantly, the DOL guidance will make it easier for employers to negotiate robust cyber protections in vendor contracts and press participants to do their share. This will be particularly helpful for employers too small for an in-house IT department and too financially stretched to hire an outside technology consultant. The DOL also appears to put most of the onus where it belongs, on service providers with the expertise and resources to deter cybercrime.

FOR PLAN SPONSORS

The DOL's "Tips for Hiring a Service Provider" run through the cyber protection questions that the plan sponsor should consider in its due diligence and standard provisions to include in the vendor contract. Examples include: what are the provider's current policies and practices and how are they updated, disclosure of any past security breaches; mandatory notification of a breach; obtaining an annual outside audit of the security practices; and commitment to comply with federal and state privacy and information security laws. I expect that many of these terms will be added to vendor's standard form contracts, especially helpful to employers without negotiating leverage to insist on contract specifics.

FOR SERVICE PROVIDERS

The second part of the DOL guidance, "Cybersecurity Best Practices" provides an annotated laundry list of steps that plan vendors should be taking to deter and respond to cybercrime. For the service provider, many of these practices are likely to already be in place. The practices also may help plan sponsors as both a due diligence checklist and an added assist in negotiating cyber protections in vendor contracts. The practices again stress the outside audit. One item not yet a best practice (but which perhaps should be) is an outside review of the software code itself to look for exploitable weaknesses.

FOR PARTICIPANTS

Online Security Tips, the third part of the tryptic, is a useful set of basic steps that participants should be taking to protect themselves. Besides the usual advice for choosing passwords and avoiding phishing attacks, it highlights the importance for all participants to establish and regularly check an online plan account (even if they prefer paper).

Counterintuitively, a participant is more susceptible to cyber fraud if he or she does not register for online access because the crooks can easily impersonate the participant and set up an account in her name. Similarly against the grain, many investment advisors counsel participants to not check on their investments too often, especially during volatile markets (think March 2020) to avoid ill-advised changes. No more. Everyone needs to periodically take a peek to check for unauthorized withdrawals or other nefarious activity.

INDEPENDENT AUDIT

The DOL reasonably stresses that providers have an independent audit of their security practices. And (less reasonably), sponsors are instructed to request and review the audit. These audit reports are hundreds of pages of technical jargon and dense information. A better approach might be for sponsors to review the "opinion" section to make sure the auditor did not find any problem. Sponsors should not be expected to analyze the intricacies of a provider's cyber security system any more than its physical security or the inner workings of their emergency power supply.

FOR RIGHT NOW

Based on the DOL's new guidance, plan sponsors should consider: reviewing vendor contracts and seeking cyber updates as needed and send the DOL tips, perhaps customized to its workforce, to all participants. Service providers should compare current practices against the DOL checklist, and make any adjustments need to conform or be able to support their own approach.

MISSING FROM THE GUIDANCE

The DOL guidance simply assumes, without citing any authority, that protecting plans and participants from cybercrime is a fiduciary duty. I agree, but more is needed on the scope of that duty and the complicated question of how much responsibility participants should bear if they are careless or ignore plan notices and benefit statements.

Or who pays if everybody did their job but someone's 401(k) account was emptied because the criminals were just smarter or luckier? The DOL also side-stepped whether participants' personal info is an ERISA-protected plan asset. Already starting to hit the courts, we can expect much litigation (and finger pointing) until there are generally accepted rules and standards of care.

As the DOL guidance implicitly recognizes, cybersecurity may be everyone's concern, but law enforcement, providers and computer experts need to lead.

The views set forth herein are the personal views of the author and do not necessarily reflect those of the law firm with which he is associated.

David E. Morse
Editor-in-Chief
K&L Gates LLP
New York, NY