Best practices for plan sponsors to address cybersecurity concerns

By
Jordan D. Mamorsky, Esq.

&

Larry E. Crocker

jijomathaidesigners / Shutterstock.com

A paradigm shift is occurring in the management and administration of retirement plans that is changing the way plan fiduciaries interact with participants. Plan sponsors are increasingly providing mandatory plan disclosures, historically delivered by mail, in electronic format to participants. Both the Department of Labor ("DOL") and the Supreme Court have recognized the shift and the resulting benefits for retirement plan administration. For example, on May 21, 2020, the DOL issued a new rule titled "Default Electronic Disclosure by Employee Pension Benefit Plans under ERISA." The rule provides safe harbor relief to plan administrators who satisfy specific conditions in delivering electronic communications. *"The Department expects the rule to enhance the effectiveness of ERISA disclosures and significantly reduce the cost and burden associated with furnishing many of the recurring and most costly disclosures."*

Also, the Supreme Court's recent decision, *Intel Investment Policy Committee v. Sulyma* noted how electronic communications can enhance participant visibility of plan disclosures. These benefits are real and, as the DOL aptly noted, will simplify plan administration and lower the associated costs. While this is an important positive effect for the employee benefits industry, the increased flow of electronic communications risks the potential exposure of participants' confidential and personal data to cybercriminals and, in turn, creates a new liability source for the plan and its service providers.

Cybersecurity concerns are particularly acute as of the publishing date of this article. In the new regulation, the DOL acknowledged heightened cybersecurity concerns: *"…the Department recognizes that increased electronic disclosures may expose covered participants' information to intentional or unintentional data breach. …the Department expects that many plan administrators, or their service or investment providers, already have secure systems in place to protect covered individuals' personal information. Such systems should reduce covered individuals' exposure to data breaches."* These comments seem reasonable; however, the DOL did not offer any guidance on specific best practices, noting that *"…efforts to establish specific, technical requirements* ***would be difficult to achieve****, given the variety of technologies, software, and data used in the retirement plan marketplace."*

The DOL's appreciation of the issue but lack of specific regulatory guidance (at least in this new regulation) only makes cybersecurity a more pressing issue for plan sponsors, particularly considering that the threat of cybersecurity breaches and the resulting liability are not going away anytime soon. As recently as April 3, 2020, a participant in the Abbott Laboratories Stock Retirement Plan filed a complaint in the U.S. District Court for the Eastern District of Illinois accusing Abbott and the plan's third-party administrator of breaching their fiduciary duties by failing to stop cybercriminals from siphoning $245,000 from the participant's account.

The increased flow of electronic communications risks the potential exposure of participants' confidential and personal data to cybercriminals and, in turn, creates a new liability source for the plan and its service providers.

Making matters even more difficult, the current economic climate is new and unprecedented. First, the COVID-19 health crisis has led to increasing unemployment and furloughs. With a loss in steady income, participants are turning to their retirement plans for cash. Second, the recent CARES Act legislation makes it easier for participants to withdraw money from their retirement account and reduces the chance of tax penalties which will likely make plan withdrawals only more popular. Finally, another challenge for plan sponsors is protecting confidential data with more employees working remotely, on remote networks, and possibly even on personal computers.

With the challenges previously mentioned, the procedures many plan sponsors, third-party administrators, and record keepers currently have in place to exchange data or manage and verify participant withdrawals may no longer be prudent or feasible. Because of the urgency in dealing with this problem, the time is now for plan sponsors, plan fiduciaries and plan service providers to address and reevaluate cybersecurity concerns—to ensure they and their participants will not fall victim to fraud, hacking or phishing schemes.

With the concerns and potential risks identified, the following questions need to be addressed by the plan sponsor:

- Has a point person been prudently selected to be responsible for an internal operational audit and external vendor procedures assessment?
- What is the point person expertise in operational compliance and vendor due diligence?
- What questions are they asking?
- What materials are they reviewing?
- What are the desired results of the audit and assessment?

ERISA has statutory protections under Section 404(a) that impose a standard of knowledge and actions as a prudent expert on plan fiduciaries as one that acts *"…with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims."* But what does that mean in the context of cybersecurity? The DOL expressly chose not to address the application of ERISA fiduciary protections stating, *"This safe harbor only establishes an optional method for delivery of covered documents. Issues pertaining to liability for security breaches are beyond the scope of this safe harbor."*

First, of course, the issue will be to identify what data is specifically misappropriated by hackers to constitute a "plan asset." The Seventh Circuit, for example, recently affirmed a district court's finding that confidential participant data including *"participants' contact information, their choices of investments, the asset size of their accounts, their employment status, age, and proximity to retirement"* could not be a plan asset because it was not property the plan could sell or lease in order to fund retirement benefits. See *Divane v. Nw. Univ.*, No. 16 C 8157, 2018 WL 2388118, at *12 (N.D. Ill. May 25, 2018), aff'd, No. 18-2569, 2020 WL 1444966 (7th Cir. Mar. 25, 2020). While it is an open issue whether participant personal data will be considered plan assets—the DOL has yet to opine on this topic—a distinction can be drawn with cases in which actual plan assets (e.g., the funds in an individual's account) are stolen by cybercriminals.

An important case in the U.S. District Court for the Eastern District of Pennsylvania, *Leventhal v. MandMarblestone Grp.* (*"Leventhal"*), underscores the prospective liability looming for plan sponsors and service providers in connec-

tion with data breaches that result in the loss of funds from participants' accounts.

Specifically, in *Leventhal*, a participant and the plan itself brought allegations against the plan's third party administrator (TPA) and custodian that they failed to enact prudent procedures and safeguards to protect the plan and participants from cybersecurity threats that resulted in cybercriminals obtaining a copy of a participant's legitimate distribution form and using that copy to submit a series of requests for fraudulent withdrawals totaling more than $400,000. The court not only found that the allegations plausibly stated the TPA and custodian were ERISA fiduciaries in connection with distributing plan assets to participants, but also that the custodian and TPA breached their fiduciary duties to the plan. See *Leventhal v. Mand-Marblestone Grp. LLC*, No. 18-CV-2727, 2019 WL 1953247, at *5 (E.D. Pa. May 2, 2019).

As ERISA fiduciaries, the *Leventhal* Court concluded that the TPA and custodian *"failed to act with the requisite prudence and diligence where they saw the 'peculiar nature' and high frequency of the withdrawal requests that were to be distributed to a new bank account, but failed to alert Plaintiffs or verify the requests"* and that Defendants failed to implement "typical" procedures and safeguards to notify Plaintiffs and/or verify the requests. This language begs the question: What are the "typical" procedures and safeguards that would have protected the service providers from liability in *Leventhal* and shielded the participant from having money stolen from their account? Plan sponsors and administrators should not take lightly or ignore the need for proper review of and diligence in its procedures.

As the retirement plan administration and management challenges continue and yet evolve, plan sponsors should expand the scope of their due diligence and take steps to identify appropriate criteria for service provider assessments. In addition, plan sponsors should also implement best practices for plan operations and compliance that meet procedural and substantive prudence requirements under ERISA. But unlike the established and streamlined procedures that meet ERISA's prudent standard of care with other fiduciary functions, the look of the process and substance in the context of data exchange and cybersecurity may need to be completely redesigned. Therefore, plan sponsors should consider a comprehensive review of their company's, and their service provider's, current data exchange and cybersecurity practices and procedures. If nonexistent, then immediate action should be taken to establish and deploy new data exchange and cybersecurity procedures. Investigation by the appointed person(s) or other plan fiduciaries should address at a minimum the following four steps:

- Review service agreements and identify any contractual indemnification provisions;
- Review all the provider's existing processes and controls;
- Review the methods for testing the sufficiency of processes and controls; and
- Substantiate the results of the assessment.

While this writing is not the place to go into the detail of a comprehensive service provider due diligence assessment, the beginning of a prudent assessment should include an evaluation of the following:

- A clearly written description of the providers and their responsibilities—including respective fiduciary responsibility
- The provider agreements—for indemnification language
- The provider's insurance coverages
- The provider's cybersecurity practices and/or policies
- The employer's internal controls and management procedures
- The employer's insurance coverages
- The results or findings of any network assessments
- Any participant training initiatives
- The benefits of an onsite visit to the provider
- The provider's Service Organization Control ("SOC") reports
    - SOC 1 report focuses on the description of a service organization's control and how controls are designed to achieve objectives
    - SOC 2 report is a review of operations, security, integrity of process, privacy, and confidentiality
- Any third-party provider certifications or assessments for quality and process standards from organizations like the Centre for Fiduciary Excellence (CEFEX), the American Institute of CPAs (AICPA), Dalbar, etc.

Clearly, the time is now for plan sponsors and service providers to swiftly address any lingering concerns over the security of data and plan assets. The effects of any failure to do so, particularly in the current economic climate resulting from the COVID-19 pandemic and the assistance response of the CARES Act, could have drastic implications, including fiduciary liability and costly insurance premiums, on top of any losses resulting from the stolen plan assets. Employers seeking to address such concerns should contact ERISA counsel or a fiduciary compliance expert to guide them through a thorough review and the implementation of necessary cybersecurity measures and data exchange procedures. NNTM