# The Uncertain Legal Landscape For Plan Fiduciaries Over Cybersecurity Challenges

*Jordan D. Mamorsky, Esq.* and *Larry E. Crocker*[*]

*It is hard to imagine that the drafters of the Employee Retirement Income Security Act of 1974 (ERISA) envisioned a day would come when retirement plans would be administered electronically and distribution of paper notices and disclosures to plan participants might become a thing of the past. However, the retirement industry seems to be swiftly moving that direction.*

There is indeed an undeniable discernable trend towards the increased flow of electronic communication with plan participants. Both the Department of Labor (DOL) and the U.S. Supreme Court have recognized the paradigm shift and the resulting benefits for retirement plan administration. On May 21, 2020, for example, 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. In their release, the DOL provided the following comments in their discussion of the new regulation:

> *The Department expects the rule to enhance the effectiveness of ERISA disclosures and significantly reduce the costs and burden associated with furnishing many of the recurring and most costly disclosures.*

Also, the U.S. Supreme Court's recent decision, *Intel Investment Policy Committee v. Sulyma,*[1] noted how electronic communications can enhance participant visibility of plan disclosures. The *Sulyma* opinion specifically suggested that plan administrators might show a participant's actual knowledge of a disclosure through obtaining electronic records that demonstrate a participant has viewed and is aware of the plan disclosure, and that this evidence could be obtained through a participant clicking to a specific plan disclosure. This aspect of the *Sulyma* decision—seemingly recommending plan administrators to employ electronic records to prove actual knowl-

[*]*JORDAN D. MAMORSKY, Esq.* is an experienced litigator and has served as counsel in well-publicized cases involving ERISA fiduciary duty and prohibited transaction matters. He regularly represents plan sponsors, plan fiduciaries, financial advisors, plan participants, company executives, third-party administrators, employers, and others in a broad range of ERISA disputes, including breach of fiduciary duty, denial of benefit, Employee Stock Ownership Plan, and deferred compensation matters. He received his Juris Doctor from New York Law School, a Bachelor of Science from Vanderbilt University, and completed a Postdoctoral Fellowship in Corporate Governance and Business Ethics at Yale University. He is admitted to practice law in New York, New Jersey, and Massachusetts. Mr. Mamorsky can be contacted at jmamorsky@wagnerlawgroup.com.

*LARRY E. CROCKER, AIFA, PRP, PPC, RF, GFS, CBFA, CPFA, L5,* is a respected industry innovator and thought leader for his knowledge of ERISA and fiduciary compliance. He is the founder and CEO of Fiduciary Consulting Group, Inc., an Independent Fiduciary firm that provides compliance consulting, operational fiduciary compliance audits, and stewardship training. The firm serves as the Named Plan Administrator and Named Fiduciary of the plan for plan sponsors across the country. The Middle Tennessee based firm serves plan sponsors, plan committees, trustees, board members, institutional clients, plan advisers and other industry service providers. He has been awarded a patent for his fiduciary compliance technology created for retirement plan sponsors and plan advisers. Mr. Crocker can be reached at 615.848.0015 or LEC@ifiduciary.com.

edge—will only encourage employers and service providers to increase the electronic footprint. Certainly, the benefits of increased electronic communications and disclosures are real and, as the DOL aptly noted, will simplify plan administration and lower the associated costs. In addition, the Supreme Court has suggested electronic communications will enhance plan efficiency. But while these are important positive effects for the employee benefits industry, the increased flow of electronic communications increases the risk of potential exposure of plan participant's confidential and personal data to cybercriminals. This 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 and have reached such a crescendo that the DOL thought it worthy to address the issue in the new regulation. The DOL commented:

> *. . . 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*." While the DOL appreciates the complexity of the challenges for plan sponsors, their lack of specific regulatory guidance in the new regulation only makes cybersecurity a more pressing issue—particularly considering that the threat of cybersecurity breaches and the resulting liability are not going away anytime soon.

As recent 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 stealing $245,000 from the participant's account. The Abbott plan is one of the largest defined contribution plans in the country, with assets close to $9.5 billion and with average participant accounts holding balances of approximately $260,000. This case underscores the urgency in enacting and complying with prudent procedures to protect the electronic security of participant accounts especially during a time where participant withdrawal requests are on the rise.

Further complicating matters, the current economic climate is new and unprecedented. First, the novel coronavirus (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 Coronavirus Aid, Relief, and Economic Security (CARES) Act legislation makes it easier for participants to withdraw money from their retirement account and reduces the chance of tax penalties, which will make plan withdrawals only more popular. Finally, more employees working remotely, and possibly on unsecure networks, creates another challenge for plan sponsors in protecting confidential data.

There is currently limited regulatory guidance on electronic data protection for retirement plans. The federal statutory guidance to ensure electronic disclosure of personal information safeguards is limited. The "Safeguard Rule" of the Gramm Leach Bliley Act of 1999 (GLBA) re-

quires that covered U.S. financial institutions safeguard sensitive data.[2] This sensitive and nonpublic information is referred to as "personally identifiable information" (PII) and encompasses items such as names, Social Security numbers, debt and payment history, and account numbers.

While the purpose of the Safeguard Rule is admirable—to ". . . *ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access* . . ."—it did not provide procedures necessary to protect such information and details. The GLBA only provides for a written security plan that calls for appointing a person or entity responsible for coordinating the security of confidential information, procedures, and protocols for designing, implementing, and testing the sufficiency of any safeguards and monitoring any service providers responsible for the safeguards. While service providers may acknowledge the responsibility in this area for their firms, the employer is left alone with its responsibility to investigate the depth and prudence of all the plan's service providers and the measures they take to safeguard the plan and participants' information.

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?

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.[3] 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 (for example, 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*),[4] underscores the prospective liability looming for plan sponsors and service providers in connection 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 the 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 the TPA and custodian were ERISA fiduciaries in connection with distributing plan assets to participants, but also found that the custodian and TPA breached their fiduciary duties to the plan and participants.

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 the 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? The same court recently raised the stakes in finding the TPA could assert a counterclaim for fiduciary breach contribution against the plan sponsor. The court specifically emphasized that "Plaintiffs' ***own carelessness*** with respect to their employees, their computer/IT systems, and employment policies facilitated and/or was the most substantial contributing factor in the occurrence of the cyber-fraud."[5] Therefore, both plan sponsors and administrators should not take lightly or ignore the need for proper review of and diligence in its procedures.

With the challenges previously mentioned, the procedures many plan sponsors, TPAs, and record-keepers currently have in place—to exchange data or manage and verify participant withdrawals—may no longer be prudent. Because of the urgency in dealing with this problem, the time is now for plan sponsors and plan fiduciaries to address and reevaluate cybersecurity practices and procedures in order 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:

- Have you prudently selected a point person responsible for an internal review of your company's practices, procedures, and operations?
- Have you established the practices and procedures to complete and external audit of your retirement plan's service providers and their data security practices and procedures?
- Does your point person have the required experience to effectively complete the above investigative analysis?

As the retirement plan operational compliance and 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 systems, processes, and procedures. If proper procedures are nonexistent, then immediate action should be taken to establish them. A comprehensive review by the appointed person or other plan fiduciaries should address at a minimum the following items:

- Review all retirement plan service agreements and identify any indemnification or limits of liability provisions.

- Review retirement plan service providers data exchange and cybersecurity processes and procedures.
- Conduct onsite visits as prudent and appropriate.
- Confirm the service providers have appropriate professional liability and cyber liability insurance coverages.
- Review the provider's Service Organization Control (SOC) reports.
    a. SOC 1 and SOC 2.

Plan sponsors, plan fiduciaries, and service providers should move swiftly to address any and all concerns over the electronic exchange of data, documents and the overall protection of plan participants confidential information that resides both internally and with plan service providers. The effects of any failure to do so, particularly in the current economic climate, the changing regulatory environment, and increasing litigation over protecting plan data and assets, could have drastic implications, including an increase in fiduciary liability resulting from stolen plan assets. Plan sponsors seeking to address such concerns should contact ERISA counsel or a fiduciary compliance expert to guide them through a thorough review of their internal controls, service agreements, service provider due diligence, and so forth. In addition, and as needed, plan sponsors should also implement necessary data exchange and cybersecurity practices and procedures.

## NOTES:

[1]Intel Corporation Investment Policy Committee v. Sulyma, 140 S. Ct. 768, 206 L. Ed. 2d 103, 2020 Employee Benefits Cas. (BNA) 69188 (2020).

[2]15 U.S.C.A. § 6801.

[3]See Divane v. Northwestern University, 2018 Employee Benefits Cas. (BNA) 186065, 2018 WL 2388118 (N.D. Ill. 2018), aff'd, 953 F.3d 980, 2020 Employee Benefits Cas. (BNA) 109900 (7th Cir. 2020).

[4]Leventhal v. MandMarblestone Group LLC, 2019 Employee Benefits Cas. (BNA) 158856, 2019 WL 1953247 (E.D. Pa. 2019).

[5]See Leventhal v. MandMarblestone Group LLC, 2020 WL 2745740, at *2 (E.D. Pa. 2020),