JOURNAL of PENSION BENEFITS

Issues in Administration, Design, Funding, and Compliance
Volume 28 • Number 2 • Winter 2021

Plan Distributions

Cybersecurity Considerations for Plan Distribution Administration

While the Digital Age has ushered in many modern conveniences, it also has raised privacy and security concerns, including in regard to the ERISA fiduciary responsibilities in relation to the cybersecurity of employee benefit plan participants' information, data, and assets. Fraudulent distribution requests are among the many risks, and this article focuses on cybersecurity best practice considerations for retirement plan distributions.

By Michelle Capezza

Michelle Capezza is a Member of Epstein Becker & Green, P.C. in the Employee Benefits & Executive Compensation practice. For more than 20 years, she has represented a range of clients in ERISA, employee benefits, and executive compensation matters including qualified retirement plans, ERISA fiduciary responsibilities, nonqualified deferred compensation arrangements, employee welfare benefit plans, equity/incentive programs, and benefits issues that arise in corporate transactions, across various industries. She also advises clients on the implications of increased automation and artificial intelligence in the workplace and the related employee benefits and compensation considerations for a changing workforce. Ms. Capezza has been recommended for her work in The Legal 500 United States and selected to the New York Metro Super Lawyers.

There is increasing scrutiny on ERISA plan fiduciaries concerning the scope of their responsibilities for the cybersecurity of plan participant personally identifiable information, data and assets, and the potential fiduciary liability that could be incurred due to a cybersecurity breach. Volumes of data and personally identifiable information (PII) related to plan participants

are collected, transmitted, processed, and stored for plan administration. With continuing advancements in plan administration technology and electronic access to account information, participant data and PII have become increasingly more vulnerable to attack as they travel through employer and third-party systems; in fact, the retirement accounts themselves are more at risk. The focus of this column is to comment solely on the plan distribution facet of the retirement plan administrative process and the cybersecurity considerations that it raises. The best practices outlined herein should be part of a larger plan fiduciary policy on cybersecurity for applicable benefit plans.

ERISA Advisory Council Reports on Cybersecurity

Several years have passed since the first ERISA Advisory Council (Council) report was issued regarding the cybersecurity risks for employee benefit plans. In 2011, the Council identified several areas of vulnerability for employee benefit plans including:

- theft of personal identities and other PII;
- theft of money from bank accounts, investment funds, and retirement accounts;
- unsecured/unencrypted data;
- outdated and low security passwords;
- hacking into plan administration, service provider, and broker systems;
- email hoaxes, including wire transfer fraud; and
- stolen laptops or data hacked from public computers where participants logged into accounts.

The 2011 Council made recommendations with respect to guidance and educational materials for plan sponsors, plan participants, and vendors.

Building upon the work of the 2011 Council, as well as the attention provided to the issue by the 2015 Council, the 2016 Council focused on outlining cyber risk management strategies. The 2016 Council created materials for plan sponsors, plan fiduciaries, and service providers to utilize when developing a cybersecurity strategy and program, including examples of questions plan sponsors and fiduciaries should pose when engaging service providers, as well as cyber insurance considerations. New guidance from the Department of Labor on cybersecurity and employee benefit plans may have been released by the time of this publication.

Within the last year, there have been at least three lawsuits related to fraudulent plan distribution requests (and one can only presume that many other incidents occur that are not publicly known). ERISA Section 502(a)(2) provides a cause of action for breach of fiduciary duty for appropriate relief under ERISA Section 409, which imposes obligations on plan fiduciaries involving the proper management, administration, and investment of fund assets. Cases are emerging that raise the question of whether participant information and data constitute a valuable plan asset that plan fiduciaries must use for the exclusive benefit of plan participants. Since *LaRue v. DeWolff, Boberg & Associates*, [552 U.S. 248 (2008)] the US Supreme Court has noted that, while ERISA Section 502(a)(2) does not provide a remedy for individual injuries distinct from plan injuries, it does authorize recovery for fiduciary breaches that impair the value of plan assets in a participant's individual account. Therefore, there is an avenue to relief under ERISA Section 502(a)(2) for harm to an individual account in a defined contribution plan. Yet, it remains to be seen how ERISA litigation in this area will evolve, including whether the equitable relief available under ERISA Section 502(a)(3) may be invoked, or whether individual claims for benefits are successfully brought in this context under ERISA Section 502(a)(1)(B).

Lawsuits Claiming Fiduciary Breach of Duty to Safeguard Plan Assets

Retirement plan fiduciaries must consider how their plan distribution administrative practices could be vulnerable to cyberattack and take note of the recent lawsuits. The following cases involving fraudulent distributions alleged that fiduciaries breached their duty by failing to establish and maintain processes to safeguard plan assets.

- In *Leventhal v. MandMarblestone Group, LLC*, [2019 WL 1953247 (E.D. Penn. May 2, 2019] the plaintiff brought a claim against the defendant after the plaintiff's 401(k) account was fraudulently reduced from almost $400,000 to $0. The plaintiff alleged that the defendant improperly distributed the funds to a bank account that was never authorized by the plaintiff, the withdrawal of this substantial amount of money was not authenticated by the plaintiff, and procedures were not implemented to notify, or request authentication from the plaintiff of these requests. The court also found on the defendant's motion to dismiss that

the plaintiff sufficiently pled a breach of duty by alleging that the defendant failed to act with the requisite prudence and diligence where the defendant saw the peculiar nature and frequency of the withdrawal requests that were to be distributed to a new bank account, but failed to alert the plaintiff or verify the requests, or to implement procedures and safeguards in connection with such requests. The court also permitted the plan administrator to assert counterclaims against co-fiduciaries for contribution and indemnification related to the complaint. [*Leventhal v. The MandMarblestone Group LLC,* Case No. 18-cv-2727, 2020 WL 2745740 (E.D. Pa. May 27, 2020)]

- In *Berman v. Estee Lauder*, [19-CV-06489 (N.D. Cal. 2019)] the plaintiff brought claims against the defendants alleging that the plan had allowed the plaintiff's $99,000 401(k) account to be fraudulently distributed to various bank accounts without the plaintiff's authorization. The plaintiff alleged that the defendants breached their fiduciary duty of loyalty and prudence by allowing the plan to make unauthorized distributions of plan assets; failing either to confirm with the plan participant the authorization for distributions before making distributions or to provide timely notice of distributions to the plan participant by telephone or email; failing to establish distribution processes to safeguard plan assets against unauthorized withdrawals; and failing to monitor other fiduciaries distributions processes. This case settled in March 2020 for an undisclosed amount.
- In *Bartnett v. Abbott Laboratories*, [Case No. 2020 CV 2127 (N.D. Ill. 2020)] the plaintiff asserted breach of fiduciary duty claims against the plan sponsor and other plan administrators seeking to recover $245,000 that was depleted from the plaintiff's retirement account in alleged unauthorized distributions by an impersonator fraudulently accessing the plaintiff's online account. The Northern District of Illinois ruled on October 2, 2020 that the third-party administrator of the retirement plan could be held liable for an ERISA fiduciary breach claim and for a claim under state law (in this case, the Illinois Consumer Fraud and Deceptive Practices Act) for failure to enact cybersecurity procedures that prevent the theft of plan assets. The court also provided the plaintiff an opportunity to amend her complaint to address the fiduciary responsibilities of the Abbott defendants. This development sounds the alarm bells regarding fiduciary status of service providers, the scope of fiduciary responsibilities, and liability exposure under ERISA and state laws (unless preempted).

These cases, and others, highlight that the retirement plan distribution process is vulnerable to bad actors, impersonators, and cyber criminals, especially when distribution requests can be processed online, on the phone, or via any means whereby there are methods to perpetrate a scam and the authentic identity of the participant or beneficiary making the request is concealed or not verified. The COVID-19 pandemic also brought renewed concerns regarding remote transactions and online hacks, phishing scams, stolen passwords, dishonest actions of former spouses or partners, and increased distribution requests via participant self-certifying procedures. As the scope of fiduciary responsibility evolves, retirement plan fiduciaries should be mindful of their potential liability for breach of their fiduciary duties by failing to establish and maintain plan distribution administrative processes to safeguard plan assets in this environment. A plan fiduciary's responsibility to act prudently and in the best interest of participants will be scrutinized whenever there are cyberattacks and/or fraudulent plan distributions, to determine whether the wrongdoing was enabled by a lack of procedural best practices. Plan fiduciaries that establish procedures to safeguard participants' data, PII, and account assets, and abide by those procedures, should experience some protection against liability for these claims.

Formulate Protocols for Plan Distribution Requests

In light of the above, and potentially many other examples of the vulnerabilities lurking in the plan distribution process, plan fiduciaries should take care to formulate and address in their overall cybersecurity best practice policies and procedures their protocols for plan distribution requests. For example, discussed below are some of the protocols that may be included.

Authentication of Identity

The administrative process for responding to distribution requests should include procedures to verify and authenticate the participant's identity in connection with the request. When requests are initiated online, over the phone, or through other electronic means, there should be at least a two-factor authentication process to confirm usernames and passwords (*e.g.*, a text of a one-time password to the participant's

phone to complete the account log-in process). The process of initiating a request might include requiring the participant to respond to a series of questions only they would be able to answer. It also should be confirmed that the distribution requests that have been placed were well-intended, such as through a verification email, phone call, or text to the participant's address and phone number on record (and using the desired method of communication pre-selected by the participant on a consistent basis). In light of recent reported cases, it would be prudent to require that a participant wait a designated period of time to receive a plan distribution when a distribution request follows a recent change in account password, mailing address, or other contact information.

It also would be prudent to determine an appropriate wait time before any funds are distributed or wired from the retirement plan to an outside account to give the plan time to receive a confirmation back from the participant in response to the verification email or text. If, at any time during the process, the proper verification and authentication of the participant and the request cannot be completed, the plan sponsor and fiduciaries should be alerted by the plan recordkeeper or other third-party administrator so that a manual process (*e.g.*, in-person or other procedure) can be implemented to confirm the request and any potential security breach can be addressed. Beneficiaries and alternate payees may be required to follow additional steps to submit required paperwork to obtain a distribution related to the participant's account. A request that participants periodically update their contact information and re-set their secure passwords and online log-in information is advisable.

Service Provider Protocols and Service Agreements

As outlined by the 2016 Council, the prudent selection and monitoring of plan service providers includes diligence of their cybersecurity procedures and safeguards, both initially when the service provider is being engaged, as well as on an ongoing basis. Plan sponsors and fiduciaries should confirm the service provider's protocols and protections related to distribution requests, including the processes to (1) authenticate the identities of those making the request; (2) confirm distribution requests; and (3) monitor any waiting periods before distributing account assets. The service provider's system and organizational controls, and processes to flag unusual requests and alert the plan sponsor and fiduciaries of potentially fraudulent activity or security breaches, should be defined and followed. Plan sponsors and fiduciaries should also determine whether they desire any enhanced administrative protocols to be added to the services, considering the procedures for plan distributions and beyond.

Once there is agreement on the plan distribution (and other) procedures being deployed, the service agreement governing the relationship should reflect adherence to the procedures as part of the service standard, along with overall terms addressing cybersecurity, breach and response procedures, indemnification, any limitations of liability, insurance for cybersecurity issues, and any loss guarantees provided by the service provider. The agreement also should provide terms for the plan sponsor and fiduciaries' receipt of initial and updated service provider Service Organizational Control reports, its ability to conduct audits of service provider systems and to receive security program updates, as well as rights to make any related requests based on an audit or review. It is important to ensure that the service provider's indemnification and service representations also cover any bad acts of its agents, subcontractors, or other third parties engaged to provide the services.

Participant Communications and Summary Plan Descriptions

Plan fiduciaries should educate employees about the importance of safe-guarding their data, PII, accounts, passwords, and PINs at all times and warn against email and phishing scams seeking to obtain this information or access. Plan participants should be encouraged to use regularly updated passwords with a high level of security and be advised to monitor their accounts. Participants should be informed of the security measures they must follow for all plan activity, including with regard to the procedures required to request plan distributions, and advised against placing too much personal information on social networking sites and reviewing sensitive data on public computers or kiosks. Participants should be advised that they need to be diligent in protecting their PII and account information, not only from cybercriminals, but also from family members or others close to them who may become estranged. Service providers may have communications on these issues that can be distributed to plan participants, or plan fiduciaries may design their own campaigns to educate participants.

Consideration also should be given to addressing the participant's role in plan cybersecurity, as well as their role with respect to the plan distribution

procedures, in the summary plan description (SPD). For example, in *Foster v. PPB Industries Inc.* [693 F.3d 1226 (10th Cir. 2012], the Tenth Circuit found that the plan administrator notified the plaintiff and other participants via the SPD of their ability to access their account information electronically and to keep their address information current, as all plan correspondence was to be mailed to their current address on file, and PIN changes and resets were always mailed to the permanent address on file. The Tenth Circuit held that the plan administrator's decision to not reimburse the plaintiff for the amount the plaintiff's ex-wife withdrew from the plan was not an abuse of discretion, because the plan administrator safeguarded plan assets, and they had been paid out in the plaintiff's name in accordance with all plan terms. The Tenth Circuit determined that the plaintiff's loss of benefits was due to the plaintiff's own failure to comply with the plan's address change requirements, as well as the fraudulent conduct of the plaintiff's ex-spouse, and to pay the plaintiff again from the plan would deplete plan assets. Based on the court's ruling in *Foster*, which rested heavily on the facts of that case, a plan may not be liable to a participant under ERISA Section 502(a)(1)(B) for denial of benefits where the plan follows procedures that are communicated to participants, and where participants are found not to have followed those procedures. Thus, it is important to delineate any required plan procedures that participants must follow, to communicate those requirements, and to ensure adherence to those procedures by the plan, service providers, and participants.

Distribution Scenarios

Plan sponsors and fiduciaries should define in their procedures any additional considerations for plan distributions that may vary depending on the common distribution scenarios for their retirement plan. For example, in-service distributions can be fraudulently initiated, but they may be more easily monitored and controlled, as the participant is actively employed and there is increased likelihood that an active participant would identify a corresponding change in their plan contributions, payroll withholdings, or they would receive a communication regarding same. Small balance cashouts, missing participants, deceased participants, online rollovers, and marriages and divorces are examples of circumstances related to distribution transactions that can easily give rise to fraud. Plan sponsors and fiduciaries may wish to consider undertaking a periodic campaign to reach out to participants to update their information, as well as to conduct a self-audit of the plan to ensure that there are no outstanding complaints or unusual and unreported problematic distribution requests to confirm that they were, in fact, processed to the correct individuals and rolled over to the correct accounts for the intended persons.

Additional Plan Fiduciary Considerations

Plan fiduciaries should periodically address cybersecurity issues and industry trends during their meetings, seek updates from their service providers on their controls and cybersecurity protocols, and incorporate cybersecurity responsibilities into fiduciary training sessions. Plan fiduciaries should ensure that they have developed and implemented an overall cybersecurity policy for benefit plans and that they review and reapprove the policy periodically. Plan fiduciaries should consider implementing specific procedures for plan transactions such as distributions, ensuring they are followed by service providers and communicated to plan participants for them to also follow. The plan procedures also should include protocols to follow in the event of a cybersecurity breach, including any parties that may need to be contacted or engaged to assist in a response. The plan fiduciaries should consider retaining service providers that may assist them in developing their policies and monitoring cybersecurity issues for the benefit plans, as well as the manner in which they will coordinate policies with the overall cybersecurity policy and leadership of their organization. Also, on an ongoing basis, it will be important to monitor changes in applicable law and related benefit plan guidance concerning such issues as overall cybersecurity measures, required disclosures and notifications, and any breach response. Plan fiduciaries also should evaluate cybersecurity insurance that may be available to protect the plan and participants and be sure to follow the requirements for such insurance to be applicable to a breach once it occurs.

Conclusion

The examples discussed are representative of the types of issues that should be addressed in, and implemented as part of, a larger cybersecurity policy for employee benefit plans. The key is for plan fiduciaries to understand their plan's vulnerabilities and take the necessary action to best protect the plans and participants. Cybersecurity risk will remain, cases will continue to emerge, and security measures will

continue to be updated and enhanced. With that in mind, it continues to be important for plan sponsors and fiduciaries to monitor plan cybersecurity practices internally within their organization and externally among service providers periodically during the plan year; address any weaknesses; educate participants on steps they should take to protect their data, PII, and accounts; and remain vigilant. ■