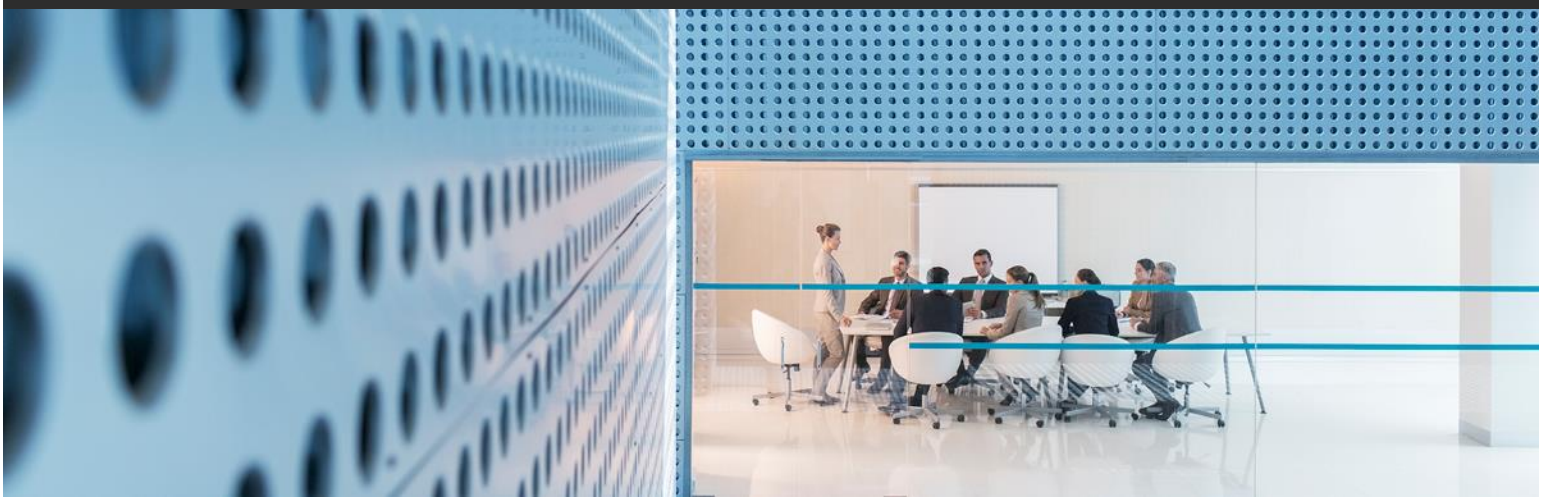
GT GreenbergTraurig

Advisory | ERISA & Employee Benefits Litigation



June 2020

Coping with the Increase in 401(k) Cyberattacks and Fraudulent Plan Distributions

Plan sponsor employers and employees participating in 401(k) or other retirement plans should be aware of cybersecurity breaches and unauthorized plan distributions. Vigilance may be even more critical because of the March 2020 CARES Act legislation that permits early retirement distributions without penalty for plan participants affected by the Coronavirus Disease 2019 (COVID-19) pandemic. The heightened level of plan distributions coupled with the security risks associated with electronic communications and the "new normal" of working remotely, sometimes on personal computers, may increase the exposure of participants' confidential and personal data to cybercriminals. While employees may envision their 401(k) plans as safely tucked away for retirement, their accounts may be vulnerable to cyber fraud.

Cyberattacks on both retirement plans and participant accounts are increasing. The attacks target 401(k) or pension information through phishing emails containing subject lines like "Changes to your 401(k) Plan" or "401(k) Open Enrollment," attempting to trick participants into revealing their 401(k) plan usernames and passwords. Some cyberattacks involve information-stealing malware that infects a victim's computer. 401(k) accounts may be particularly vulnerable to fraud because account holders may not interact with them frequently. The hands-off nature of 401(k) plans may make them an attractive target

for cybercriminals who are drawn to the large pool of assets and lack of daily attention. Additionally, plans are only required to mail statements quarterly, and participants are generally advised to leave their 401(k) accounts alone.

Plan Sponsor Liability

Under privacy and data-security laws, responsibility for proper collection, storage, and use of plan participants' personally identifiable information (PII) rests with the entity that ultimately controls the decisions regarding such activities (referred to as the "data controller"), which in the case of a 401(k) or other retirement plan is the employer plan sponsor, or trustees in the case of a multi-employer plan. While financial responsibility for failure to comply with data protection and privacy laws can be shifted by contract as between a data controller and a third-party vendor, legal liability to an individual whose PII has been improperly collected, stored, used, or transferred remains with the data controller.

Thus, based in part on trends in regulatory enforcement and litigation following headliner data breaches, and in view of ERISA's strict fiduciary requirements, a court may find that the employer plan sponsor or trustees have a fiduciary duty to protect plan participants' PII based on a plan fiduciary's duty to prudently administer the plan.

Although it is best practice for the employer plan sponsor or trustees to transfer to a service provider (e.g., plan administrator), through contractual indemnification provisions, any resulting financial liability for failure to safeguard the plan participants' PII, the plan sponsor is still exposed based on independent duties they owe the plan participants under ERISA and the compliance obligation belonging to the data controller under most privacy laws. In assessing whether compliance obligations have been met, courts have focused on the standard of care followed by fiduciaries during the course of: (i) vendor selection and (ii) monitoring the vendors' activities following selection. Under ERISA, any finding that plan fiduciaries breached the applicable standard of care may result in personal liability for losses attributable to that breach.

Emerging Litigation

Participant litigation against an employer and plan administrator for 401(k) plan distribution fraud was settled in March 2020.[1] Terms of the settlement were not disclosed. According to the complaint, there were numerous security lapses by the plan administrator and the employer that resulted in the failure to identify and halt suspicious distribution requests, such as requests for multiple distributions to accounts in different banks, and to confirm authorization for distributions with the plan participant before making distributions. The complaint does not mention the exact mechanism by which the fraudulent transfers happened. It is unclear whether the persons responsible were relatives of the plan holder, insiders at the firm managing the 401(k), or unrelated cyber criminals.

Another employer and the same plan administrator are currently in litigation with a participant in an Illinois district court for 401(k) plan cyber fraud.[2] According to the complaint, an unknown user accessed the participant's account online, changed the password, and initiated a transfer to a new bank account, after getting additional personal information from the plan administrator's customer service representatives. The participant further alleges that her employer and the plan administrator ignored basic security protocols in their interactions with the fraudster, from failing to enforce a security question

[1] *Naomi Berman v. Estee Lauder Inc.* (USDC, W.D. Cal.) Case No. 3:19-cv-06489, filed Oct. 9, 2019.
[2] *Barnett v. Abbott Laboratories*, Illinois Northern District Court, 1:20-cv-02127, filed April 3, 2020.

routine to giving out her complete home address over the phone. According to the participant, she never shared her password and had requested to be notified by email of any changes to her account.

The participant had about $362,511 in her 401(k) plan at the end of 2018. By the next month, $245,000, about two-thirds of her retirement, was gone. According to the complaint, the fraudster, whose IP address was registered to a user in India, changed the password and added a new bank account to the participant's online profile in late December 2018. But the imposter, who several times pretended to be the participant, was unable to complete the distribution until calling the employer's benefits center, which was staffed by plan administrator customer service representatives. The participant has recovered $48,991 in taxes withheld from the fraudulent withdrawal and $59,494 from a bank account created by the fraudster, according to the complaint. The lawsuit seeks the full balance, plus damages, including any lost income and expenses associated with the lawsuit.

On April 6, 2020, the DOL filed a petition in the Illinois Northern District Court seeking to compel the plan administrator to turn over documents in an investigation that commenced in July 2019.

The plan administrator sued in the above two cases is currently under DOL investigation for allegedly processing unauthorized retirement plan distributions made through cybersecurity breaches.

Plan Administrator and Custodian Liability for Cybersecurity Theft of Participant Accounts

A participant and his 401(k) profit sharing plan sued the plan administrator and custodian in a Pennsylvania district court for breach of fiduciary duty under ERISA, claiming the administrator and custodian failed to establish prudent procedures to protect the plan and participants from cybersecurity theft.[3]

According to the complaint, subsequent to the participant's withdrawal of $15,000 from his plan account, "unknown criminal(s)" obtained a copy of the participant's original withdrawal form by using an "unknown method of cyber-fraud possibly relating to the electronic transmission of that form."

Thereafter, according to the complaint, these criminals "posed electronically" as the participant's office administrator and sent fraudulent withdrawal forms to the plan administrator and custodian requesting the transmittal of funds to a bank account that did not belong to the participant. As a result of the fraudulent withdrawal requests, the participant's account in the plan was depleted from more than $400,000 to $0.

The district court concluded that the plan administrator is a fiduciary primarily because it was explicitly designated as the "named fiduciary for purposes of ERISA" in the plan administration agreement. The district court also decided that the custodian is a fiduciary since the agreement provided it with "general administrative responsibilities" that include the ability to "[t]ake all other acts necessary for the proper administration of the Account" and the fact that it had the ability to dispose of plan assets is distinguishable from a bank that only receives deposits for the plan.

The district court not only found the plan administrator and custodian were ERISA fiduciaries in connection with distributing assets to participants but also found that they breached their fiduciary duties to plan participants since they failed to act with the requisite prudence and diligence when they saw the "peculiar nature" and high frequency of the withdrawal requests that were to be distributed to a new bank

[3] *Leventhal v. MandMarblestone Grp. LLC*, United States District Court for the Eastern District of Pennsylvania, Civil Action No. 18-cv-2727, decided May 1, 2019.

account but failed to alert the participant or verify the requests. Moreover, the court emphasized that the plan administrator and custodian failed to implement "the typical procedures and safeguards" used to notify the participant of the strange requests and/or verify the requests.

Finally, it is important to note that the court dismissed the argument that the contract provisions of the agreement declaiming liability precluded recovery for breach of fiduciary duty, since such waivers of fiduciary duty are prohibited by ERISA. Under ERISA, the court said, any provision in an agreement or instrument which purports to relieve a fiduciary from responsibility or liability for any responsibility, obligation, or duty under ERISA is void as against public policy.

DOL Guidance

Within the context of privacy and security concerns, the management of third-party service providers has been recognized by the DOL ERISA Advisory Council as one of the major areas of vulnerability that challenges plan fiduciaries. In this regard, the Council recommended that due diligence about plan data security in the selection and monitoring of service providers (including TPAs) should include at least the following topics:[4]

- What are the service provider's processes and systems for dealing with cybersecurity threats and protection of personally identifiable information?
- Does the company have a privacy and security policy, and does the policy apply to data held by benefit plans?
- Is the company's policy clear with respect to storing personally identifiable information on laptops and portable storage devices? What is that policy?
- Is advanced authentication used by the company? Can the service provider explain the process? Can you explain it?
- Are technology systems regularly updated?
- Does the service provider have policies on storing personally identifiable information including where it is stored, how long it is stored, and how it is eliminated?
- Are all personnel who come in contact with personally identifiable information trained on adequate protection of the information?
- Does the company carry cybersecurity insurance?
- Has the company experienced any security breaches?

Conclusion

Fulfillment of the fiduciary duty to monitor will help plan fiduciaries meet their obligation of procedural prudence under ERISA. Monitoring of the cybersecurity controls of third-party service providers, particularly the plan administrator, should occur on a regular basis and should be documented and involve experts if necessary (e.g., a periodic assessment conducted by counsel. The plan fiduciaries should

[4] DOL ERISA Advisory Council Report, "Cybersecurity Considerations for Benefit Plans," dated November 2016, published Feb. 27, 2017.

also make informed and reasoned decisions based on information they gather through monitoring activities.

Author

This GT Advisory was prepared by:

- Jeffrey D. Mamorsky | +1 212.801.9336 | mamorskyj@gtlaw.com