COMPLIANCE CONSULT Published in PLANADVISER November-December 2019

Cyberfraud

Must a plan's security policies meet the duty of prudence?

By David Kaleda

Art by Tim Bower

Criminals attempting to steal employees' benefits is not a new issue. However, the means by which they commit such crimes have changed with the advancement of technology and how benefits are paid. Two recent cases alleging breach of fiduciary duty under the Employee Retirement Income Security Act (ERISA) in connection with the distribution of participant account balances in defined contribution (DC) plans highlight the compliance and litigation risks associated with plan losses.

On October 9, a plan participant filed a complaint in the case styled *Renaker v. Esteé Lauder Inc.* In that case, the participant learned that her plan had paid approximately $90,000 in distributions from her account to three bank accounts that did not belong to her. The participant alleged that the plan sponsor, recordkeeper and directed trustee failed to meet the duty of prudence under Section 404(a)(1)(B) and the duty of loyalty under ERISA Section 404(a)(1)(A).

The participant in the *Esteé Lauder* complaint pointed to deficiencies in the plan's policies and procedures that led to the plan making unauthorized distributions. For example, the participant stated that the defendants should have 1) confirmed that the participant authorized the distributions before making them; 2) provided to the participant timely notice of the distributions so she could have recognized the fraud; and 3) identified and halted suspicious distribution requests. The plaintiff states that requests for multiple distributions to be paid to accounts held at different banks should have alerted the defendants that the distribution requests were possibly fraudulent. The plaintiff also argued that the defendants failed to monitor each other's distribution policies and procedures and the processing of distribution transactions. The litigation is in its early stages. It remains to be seen how the court will view these allegations.

In *Leventhal v. MandMarblestone Group LLC*, the plaintiff filed a complaint seeking relief similar to that requested by the participant in *Esteé Lauder*. Leventhal was a participant in a 401(k) sponsored by his employer. Over a period of time, the plan distributed $400,000 based upon fraudulent withdrawal forms submitted to the plan administrator by unknown persons. Interestingly, the participant used the withdrawal forms required by the plan administrator to request a $15,000 distribution, which the plan paid to him. However, the unknown persons somehow obtained a copy of that withdrawal form using an "unknown method of cyberfraud possibly relating to the electronic transmission of [the original] form." The fraudsters sent to the plan administrator withdrawal forms from an address that appeared to be from the participant's employer. On those forms, the fraudsters requested that the payments be made to a bank account that was different than the one to which the plan paid the $15,000.

The court in *Leventhal* has not yet concluded that a fiduciary breach occurred. However, it held that the facts could result in a determination that the defendants breached their duties of prudence, and thus it refused to dismiss the complaint. In so doing, the court rejected a defendant's argument that there is no duty under ERISA to prevent forgeries. The court also held that the plaintiffs established, at least at this point in the litigation, that the third-party administrator (TPA) and custodian acted as fiduciaries in connection with the payment of the distributions. This is notable because most TPAs and custodians do not act as fiduciaries, and several courts agree.

Esteé Lauder and *Leventhal* illustrate the compliance and litigation risks to which an adviser, the adviser's affiliates, plan service providers and plan sponsors may be subject when administering and managing an ERISA-covered plan. The Department of Labor (DOL) has not issued specific guidance on how to address frauds perpetrated against employee benefit plans or what kind of measures a plan must have in place to address threats to the security of its assets. However, ERISA requires that a fiduciary discharge his duties "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."

Advisers, adviser affiliates, plan service providers and clients of any of them should consider whether their policies and procedures for protecting the security of plan assets will allow the plan fiduciaries to meet the duty of prudence. Additionally, they

should be aware that the DOL will likely look into whether it should publish guidance in this area. Benefit-plan-market participants should take the opportunity to help the DOL craft sensible guidance that balances the need to protect plan assets and the requirements of ERISA.

While the duty of prudence would appear to require policies to protect assets from fraudsters, ERISA does not demand that they be foolproof. Guidance should recognize that participants play a role in protecting their plan benefits.

David Kaleda *is a principal in the fiduciary responsibility practice group at Groom Law Group, Chartered, in Washington, D.C. He has an extensive background in the financial services sector. His range of experience includes handling fiduciary matters affecting investment managers, advisers, broker/dealers, insurers, banks and service providers. He served on the DOL's ERISA Advisory Council from 2012 through 2014.*

Tagged: employee benefits, ERISA litigation, retirement plan cybersecurity