## LEGAL UPDATE

# Cybersecurity and Retirement Plans: What Plan Sponsors Should Do

Marcia S. Wagner, Esq.

Cybersecurity breaches of retirement plan participant accounts have occurred with increasing frequency in recent years. Just this past April, a plan participant filed a complaint alleging ERISA breaches of fiduciary duty and violations of the Illinois Consumer Fraud Act against Abbott Laboratories, the plan sponsor, and Alight Solutions, the plan's third party administrator and recordkeeper, for unauthorized distribution from a plan in the amount of $245,000. The suit followed a Department of Labor investigation into the cybersecurity practices of Alight Solutions which, according to the DOL, had processed unauthorized distributions as a result of cybersecurity breaches relating to its ERISA plan clients' accounts. The Abbott case and other recent suits against plan sponsors, including a complaint against Estee Lauder last year, raise the question: What can plan sponsors do to minimize their fiduciary liability for cybersecurity breaches?

So far, the DOL has not taken a formal position or issued comprehensive guidance on the ERISA fiduciary standards governing retirement plan cybersecurity, including what data is a "plan asset." Even when fiduciaries are equipped with such guidance, however, the analysis will likely be highly fact-specific and contingent on the specific data actually misappropriated by hackers. 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. Northwestern. Univ.*, No. 16 C 8157, 2018 WL 2388118, (N.D. Ill. May 25, 2018), aff'd, No. 18-2569, 2020 WL 1444966 (7th Cir. Mar. 25, 2020). When the actual funds in an individual's retirement account are stolen, however, ERISA's fiduciary protections will apply and HIPAA responsibilities will also apply if the breach involves unauthorized access to Protected Health Information (PHI). The question then becomes, who will be liable when plan assets are stolen and what do fiduciaries need to do to protect themselves from liability?

The DOL's 2002 regulations pertaining to electronic disclosure of plan information to participants instructed plan administrators to take "appropriate and necessary measures reasonably calculated to ensure that the system for furnishing documents …[p]rotects the confidentiality of personal information relating to the individual's accounts and benefits (*e.g.*, incorporating into the system measures designed to preclude unauthorized receipt of or access to such information by individuals other than the [participant])." In the same vein, the DOL's recently released proposed regulations on electronic disclosure require "the administrator [to] take measures reasonably calculated to ensure that the website protects the confidentiality of personal information relating to any covered individual." This language, however, does not explain how to satisfy this obligation, nor is it dispositive as to a plan sponsor's fiduciary obligations.

Without substantive regulatory guidance and taking into account the increasing threat of cyber-criminality to retirement plans, plan sponsors should establish, evaluate, and test their cybersecurity protocols. Plan sponsors might want to take a conservative approach and assume that ERISA's duties of loyalty and prudence do indeed apply to participants' identification data and their plan benefits in case the DOL or the courts conclude such information do constitute "plan assets" for purposes of ERISA. Employers should consider taking the following steps to protect their plans from potential cybersecurity breaches:

- Request information from service providers with whom participant data is shared regarding their data security processes and data transmittal policies;
- Review and revise, as necessary, service agreements with the plan's service providers and negotiate to add provisions including: (i) a commitment to maintain cybersecurity insurance at a particular level, (ii) indemnification of the plan for losses, damages, expenses and lawsuits arising out of unauthorized access to participant data, (iii) an agreement to implement specified standards of cybersecurity, and (iv) an agreement as to how and when the plan sponsor will be notified in the event of a data breach;
- Review and modify, as necessary, the plan's fidelity bond to ensure that coverage is sufficient for the potential risks, and add optional coverages for depositor's forgery, computer fraud, and funds transfer fraud;
- Acquire cybersecurity insurance;
- Acquire or review fiduciary liability insurance to determine if it covers fiduciary breach claims related to selection and retention of plan service providers;
- Undergo a "data diet," which involves a review of participant data that is currently shared to ensure that the minimum possible amount of data is shared; and
- In the event plan services are put out to bid, ensure that the requests for proposals seek sufficient information about candidates' data security and data transmittal policies, insurance coverage, etc.

As is true of ERISA prudence considerations generally, there is no one-size-fits-all approach. Note that some of the same considerations that apply to implementing an investment strategy would be equally applicable in the cybersecurity context. For example, if the fiduciaries believe that they lack the requisite knowledge in this area, they should hire a cybersecurity expert. Similarly, in the same way that fiduciary training is recommended for plan fiduciaries, internal training may be appropriate with respect to cybersecurity risks for all individuals who have access to personal identifying information.

**Marcia S. Wagner** *is the Managing Director of The Wagner Law Group. She can be reached at 617-357-5200 or* Marcia@WagnerLawGroup.com.