DORSEY
DORSEY+WHITNEY LLP

Is Data the Next Frontier in ERISA Litigation?

January 4, 2021 – Dorsey Health Law
by Alan J. Iverson, Stephen P. Lucke, and Robert Cattanach

Health and retirement benefit plans subject to the Employee Retirement Income Security Act ("ERISA") have troves of personal information regarding plan participants and their beneficiaries—*e.g.*, participants' age, marital status, personal assets, medical and prescription drug claim data, and medical history. Although the Health Insurance Portability & Accountability Act ("HIPAA") regulates treatment of protected health information, ERISA does not expressly address how plan fiduciaries may have a responsibility with respect to participants' personal data or personally identifiable information ("PII").

Nevertheless, one emerging trend in ERISA litigation is lawsuits arguing that ERISA's duties of loyalty and prudence, among other ERISA duties, impose a duty to protect participants' privacy. These lawsuits often argue that participants' data is a "plan asset" that, when used or disclosed improperly, gives rise to claims for breach of fiduciary duties and other claims under ERISA. Plan sponsors and fiduciaries should pay attention to this developing area of law and be proactive to ensure that their actions do not put participants' personal information at risk, and be able to demonstrate that reasonable steps have been taken to protect such data.

I. ERISA Duties Regarding Plan Assets

ERISA imposes several duties on plan fiduciaries with respect to their use of plan assets. ERISA requires that plan fiduciaries act for the "exclusive purpose" of providing benefits to participants and beneficiaries. 28 U.S.C. § 1104(a)(1)(A). ERISA requires that fiduciaries act "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 . . ." *Id.* § 1104(a)(1)(B). ERISA also prohibits plan fiduciaries from engaging in

Related People

- Alan J. Iverson

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

certain prohibited transactions, including transactions between the plan and certain related parties, also known as parties in interest, which the fiduciary knows constitute a direct or indirect transfer to, or use by or for the benefit of, a party in interest, of any assets of the plan. 29 U.S.C. § 1106(a)(1).

II. ERISA Liability for Fraudulent Distributions of Plan Assets

When participants' money is fraudulently withdrawn from their' benefit accounts, they have sued plan fiduciaries for breach of fiduciary duty. For example, in *Leventhal v. MandMarblestone Grp., LLC*, a law firm partner brought an ERISA fiduciary breach claim against a plan administrator for approving fraudulent distributions from his 401(k) account. 2019 U.S. Dist. LEXIS 74123, at *7-17 (E.D. Pa. May 1, 2019). The court ruled that the claim survived dismissal because the plaintiff sufficiently alleged that the defendant failed "to act with the requisite prudence and diligence" when it did not alert plaintiff or institute other safeguards to protect against the fraudulent withdrawal requests. *Id.* at *15-17. A similar claim against the operator of a plan's benefit center and website survived dismissal in *Bartnett v. Abbott Labs.*, 2020 U.S. Dist. LEXIS 182645, at *18-19 (N.D. Ill. Oct. 2, 2020). These cases follow a familiar trend—lawsuits seeking to recover money that was stolen as a result of a data or cybersecurity lapse. Recent case law, however, suggests that fiduciaries may face ERISA claims for the improper use or disclosure of participant data itself, regardless of whether that data is used to make a subsequent fraudulent distribution.

III. Is Participant Data Itself a "Plan Asset"?

ERISA does not specifically define "plan assets," but states that "'plan assets' means plan assets as defined by such regulations as the Secretary [of Labor] may prescribe." Those regulations define certain categories of "plan assets"—for example, "plan investments" (*See* 29 C.F.R. §§ 2510.3-101(a)(2)—but the Department of Labor has stated that "in situations outside the scope of the plan assets-plan investments regulation (29 C.F.R. § 2510.3-101), the assets of a plan generally are to be identified on the basis of ordinary notions of property rights under non-ERISA law." *See, e.g.*, Advisory Opinion 1993-14A. The question, therefore, is whether participant data is a plan asset under those "ordinary notions of proper rights."

Whether participant data is a plan asset is currently the subject of debate. On one hand, two recent court-approved settlements suggest that participant data may be viewed as plan asset. In *Cassell v. Vanderbilt Univ.*, the university paid $14.5 million to settle breach of fiduciary duty and prohibited transactions claims premised on the plan's recordkeeper's use of participant data to market and sell additional services to the plaintiffs. *See* Second Amend. Compl., ¶¶ 279-82, No. 16-cv-02086 (M.D. Tenn. June 6, 2018), ECF No. 102. The settlement required the plan's current recordkeeper to refrain from using participant data to market or sell products or services to plan participants. *See* Class Action Settlement Agreement § 10.6, No. 16-cv-02086 (M.D. Tenn. April 23, 2019), ECF No. 147-1. Another lawsuit alleging similar claims settled for $14 million and the settlement agreement contained a similar prohibition on the use of participant data to cross sell other products. *See* Class Action Settlement Agreement § 10.8, *Kelly v. Johns*

Hopkins Univ., No. 16-cv-02835 (D. Md. Aug. 6, 2019), ECF No. 84-2.

On the other hand, at least one court has ruled that participant data is not a "plan asset." In *Divane v. Northwestern Univ.*, plan participants alleged that the university breached its fiduciary duties and engaged in prohibited transactions when it allowed the plans' recordkeeper to access participant data and use it to sell products to them. 2018 U.S. Dist. LEXIS 87645, at *36-37 (N.D. Ill. May 25, 2018), *aff'd on other grounds*, 953 F.3d 980 (7th Cir. 2020). The court rejected those claims, ruling that although "a compilation of the information [the recordkeeper] has on participants has some value . . . the Court cannot conclude that it is a plan asset under ordinary notions of property rights." *Id.* at *38-39. The court emphasized that no court has yet recognized such a right, and that participant data was not "property the plan could sell or lease in order to fund retirement benefits." *Id.*

While *Divine* may have been the first court to rule on the issue, it will not be the last. The issue of whether participant data constitutes a plan asset is also pending in *Harmon v. Shell Oil, Co.*, a case before the United States District Court for the Southern District of Texas. There, plaintiffs allege that the plan recordkeeper used (or could use) participant data to convince them to move their funds into higher cost, lower performing investments rather lower cost, better performing investments. *See generally* Am. Compl., 20-cv-00021 (S.D. Tex. May 21, 2020), ECF No. 84. According to the plaintiffs, that conduct amounts to a breach of fiduciary duties and prohibited transactions.

In opposing dismissal, plaintiffs argue that participant data is an "asset" because it amounts to "intimate knowledge of financial and personal information combined with insider knowledge of exploitable triggering events," such as retirement and marital status. Opp'n to Defs.' Mot. to Dismiss at 14-15, 20-cv-00021 (S.D. Tex. June 6, 2020), ECF No. 93. Further, Plaintiffs argue that since this information "is collected by the Plan for the exclusive purpose of administering the Plan and providing benefits to participants," it is a *plan* asset. *Id*. Plaintiffs also argue that the definition of "plan asset" includes participant data. *Id.* at 15-17.

These cases are likely only the opening salvo of litigation regarding ERISA fiduciaries' duties with respect to participant data. While the cases have primarily involved retirement benefit plans, they have implications for fiduciaries of health benefit plans regulated by ERISA as well. In addition to potential ERISA claims arising from data breaches or cybersecurity lapses, health plans may face ERISA claims regarding their use of participant data. Although the law in this area is still emerging, to minimize exposure ERISA fiduciaries should ensure that they are taking appropriate steps to protect participant data.

There are many steps ERISA fiduciaries can take to safeguard participant data, including:

- Develop cybersecurity policies, including both procedures to prevent improper use or disclosure of participant data as well as an Incident Response Plan to execute in the event of a breach;

- Review agreements with third-party service providers to ensure they appropriately limit the use of participant data and mandate proper cybersecurity practices;
- Improve data security protocols to minimize the likelihood of unauthorized access to or use of participants' data; and
- Consider obtaining cybersecurity insurance that will provide coverage in the event of a breach or other improper use of participant data.

It may be too much to expect that participant data can be perfectly protected under all circumstances, especially given the almost ubiquitous attacks by cyber criminals, but ERISA fiduciaries would be well served to be able to demonstrate that reasonable steps were taken to provide data security, and that procedures were in place to respond to any unauthorized disclosure.