Bloomberg Law

The United States Law Week

# INSIGHT: Data Privacy and Cybersecurity—What's a Plan Fiduciary to Do?

By Allison Itami, David Levine, George Sepsakos, and Kevin Walsh Posted June 12, 2019, 4:00 AM

The recent Vanderbilt University retirement plan settlement had unusual provisions regarding privacy and security of data and should catch the attention of ERISA plan fiduciaries. Attorneys from Groom Law Group, Chartered, examine recent cases showing data privacy and security are moving center stage.

Data privacy is an emerging area for ERISA plan fiduciaries. And the rules aren't all that clear.

The issue of data privacy made news May 31 when the U.S. District Court for the Middle District of Tennessee granted conditional approval for Vanderbilt University to settle claims related to its 403(b) plan for $14.5 million dollars. The settlement also had non-monetary conditions including a prohibition on Vanderbilt letting its next recordkeeper use plan data to cross-sell additional products and services to plan participants without their affirmative consent.

This case raises many questions for plan fiduciaries. What are plan fiduciaries to do when it comes to protecting the data of the plan's participants? Is participant consent required? Should data be considered like any other form of service provider compensation? Should fiduciaries know what data their plan gathers, who it is shared with, and how it is used?

All of these questions are evolving as plaintiffs begin to probe these issues. In the past year, three big cases have signaled that data privacy and cybersecurity are moving to center stage.

**Data Privacy**

On the ever-evolving topic of privacy, two cases provide conflicting views on the responsibilities of plan fiduciaries over plan data and participant information. The trend they signal is that courts are being asked to decide the question. There have already been signals that plaintiffs' counsel is considering data use as an issue when preparing complaints.

In *Cassell v. Vanderbilt Univ.*, No. 3:16-cv-02086, (M.D. Tenn.), Vanderbilt has agreed to pay $14.5 million to resolve a variety of claims brought in the case, including one based on the plan's recordkeeper's use of participant data.

Plaintiffs alleged that the recordkeeping pricing failed to take into consideration "the value of the vendors' access to Plan participants and their data for marketing purposes." While denying the claims, Vanderbilt agreed that with respect to future recordkeeping contracts, "[t]he Plan's fiduciaries shall contractually prohibit the recordkeeper from using information about Plan participants acquired in the course of providing recordkeeping services to the Plan to market or sell products or services unrelated to the Plan to Plan participants unless a request for such products or services is initiated by a Plan participant."

Additionally, as part of the settlement agreement, Vanderbilt must inform its current recordkeeper to "refrain from using information about Plan participants acquired in the course of providing recordkeeping services to the Plan to market of sell products or services unrelated to the Plan to Plan participants unless a request for such products or services is initiated by a Plan participant."

This settlement follows on a decision in 2018 in *Divane v. Northwestern Univ*., 1:16-cv-08157 (N.D. Ill., 2d. Amended Compl. filed July 12, 2018). There, the district court held that participant data is not a plan asset and dismissed the case.

The court in *Divane* opined that the participant information was not a plan asset under ordinary notions of property rights. It stated that the data was not "property the plan could sell or lease in order to fund retirement benefits." Additionally, the court considered whether there was any allegation that the plaintiffs could sell their personal information for value and characterized the issue as a privacy right rather than a property right. The *Divane* case is currently being appealed to the Seventh Circuit.

**Cybersecurity Concerns**

Along with seeking to ensure privacy, it is also important to protect data. Cybersecurity can be loosely defined as the techniques used to protect the integrity of networks, programs and data from attack, damage, or unauthorized access. Fraudulent distribution requests that are facilitated through a network or that use participant information electronically obtained without authorization are among the most common examples of cyber incidents that a retirement plan may face.

A federal district court in Pennsylvania recently rejected a motion to dismiss filed by defendants who sought to avoid liability for fraudulent distributions from a plan caused by cyber criminals.

In *Leventhal v. MandMarblestone Grp. LLC* (2019 BL 158856, E.D. Pa., No. 2:18-cv-02727), the district court held that the plaintiffs sufficiently pled that the defendants, the third-party plan administrator and the plan custodian, breached their alleged "fiduciary" duty by permitting the distribution of plan assets to "cyber criminals."

Although the decision will not be the last on whether plan service providers have responsibility to protect against cyber criminals (and the decision is likely not even the last decision in the case given a likely debate about the fiduciary status of the providers themselves), the case likely represents the first salvos in determining how risk is borne between plan fiduciaries, service providers, and participants when plans are the victims of cyber crimes.

In *Leventhal*, it was alleged that cyber criminals obtained a copy of a participant's legitimate distribution form, possibly in connection with the initial electronic transmittal of the form and used that copy to submit a series of requests for fraudulent withdrawals totaling more than $400,000.

The plaintiffs alleged the requests came from criminals that "posed electronically" as the plan sponsor point of contact using an email account that appeared to be the sponsor's office email account. The distributions were made to a bank account the participant allegedly had never previously used for distributions.

The plaintiffs alleged that the defendants did not "implement[] the commonly employed procedures and safeguards used to notify plaintiffs of these strange requests and/or verify the authenticity of the requests." The plaintiffs also alleged that the plan administrator was aware of the peculiarity [and frequency] of the requests, but did not voice any its concerns to the plan custodian.

The court found the defendants were fiduciaries and concluded the facts pled were sufficient to allege that plan fiduciaries had failed to 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 in the conduct of an enterprise of a like character and with like aims," under ERISA section 404(a).

Specifically, the court was concerned that defendants should have recognized "the peculiar nature and high frequency of the withdrawal requests that were to be distributed to a new bank account," and as a result the plan fiduciaries should have "alert[ed] plaintiffs or verif[ied] the requests."

While only a decision on a motion to dismiss, this case raises concerns that plaintiffs will increasingly assert that the steps plans and service providers have been taking with respect to cybersecurity—even though there are very limited legal standards that actually apply—may not be enough going forward.

**What's a Fiduciary and Service Provider to Do?**

This area is evolving rapidly and there is no silver bullet. Today, it may make sense to begin to take steps to understand how a plan is operating. These steps may take the form of evaluating fees in light of data use, it could involve developing cybersecurity guidelines, it could include data tagging, or it could take some other form.

If you haven't begun to see these as issues that impact your plan and/or services, now may be a good time to refocus. As technology evolves, the law has struggled to keep up with data usage and cybersecurity. With these new cases, plans and service providers should be aware that the law is catching up.

*This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.*

**Author Information**

*Allison Itami, David Levine, George Sepsakos, and Kevin Walsh are principals at Groom Law Group, Chartered. Each advises plan fiduciaries and service providers on a variety of topics including data privacy, cybersecurity, and applicable standards of care.*

**Related Articles**

Vanderbilt Can Settle Retirement Plan Suit for $14.5 Million (May 31, 2019, 7:02 AM )