PUBLICATION

Fiduciary Risk in a Financial Wellness World

Robert R. Gower

As financial wellness programs and the related cross-selling of products continue to expand in design and popularity, ERISA fiduciary considerations continue to mount. When recordkeepers and other service providers expand their offerings (or partner with an external party to support financial wellness initiatives), they often rely on the rich resource of participant data that they have collected to market their products. The concept is not new—recordkeepers have a long history of using participant data to market additional services and products, often as beneficial tools for participants. With recordkeepers and other non-fiduciary service providers having financial incentives to sell financial wellness products using the data they collect, plan fiduciaries need to pay attention to such sales activity and the participant data being used as part of the marketing process. A lawsuit filed in the United States District Court for the District of New Jersey is reminding ERISA plan fiduciaries that failing to do so may create significant fiduciary risk.

The lawsuit, *Williams-Linzey v. Empower Advisory Group, LLC,* alleges that Empower improperly and repeatedly leveraged its position as a retirement plan recordkeeper to harvest highly confidential, private financial data concerning retirement plan participants for its own economic benefit. Specifically, the lawsuit claims that Empower used the data it collected to identify retirement plan participants with large account balances nearing retirement age and target them for Empower's managed account program. The complaint alleges that the targeted campaign falsely portrayed the managed account program as a superior investment option, despite its "extremely high costs" and regardless of whether it was actually in the best interest of participants, all for Empower's financial gain.

The complaint offers a legal theory that is yet to be well addressed in ERISA case law—that participant data should be treated as a "plan asset" subject to ERISA's fiduciary duties of prudence and loyalty. Under this theory, Empower would not only be held to a fiduciary standard based on its provision of investment advice, but also for its control and exercise of discretion over an alleged plan asset—that is, participant data. And while Empower is the only defendant in the case, the complaint also asserts that the plan fiduciaries breached their own fiduciary duties by failing to monitor Empower's use of participant data. Such an assertion highlights the real-world risk of permitting recordkeeper utilization of participant data for any purpose beyond core recordkeeping responsibilities, regardless of whether the use may be beneficial to participants. This article provides practical contracting considerations for plan fiduciaries seeking to strike a balance between fiduciary risk and permitting financial wellness products.

Understanding the Risk

Data mining has undoubtedly become the gold rush of the 21st Century. In the right hands, data has the ability to influence thought and behavior and therefore create significant financial profits. Under section 404(a) of ERISA, fiduciaries must discharge their duties with respect to a plan solely in the interests of providing benefits to participants and beneficiaries, and only paying reasonable expenses for plan administration (the "duty of loyalty"), and in carrying out these responsibilities, must act with care, skill, prudence and diligence under the circumstances (the "duty of prudence"). As such, it is incumbent on plan fiduciaries to scrutinize the use of data collected by ERISA plan service providers, particularly with respect to use of the data to market additional products where there is a profit to be made (regardless of whether the additional products are ERISA plans). Failure to do so could lead to complaints from participants that they were marketed or sold unreasonably expensive or ineffective products and services at a profit to the service provider (similar to the allegations in *Williams-Linzey*). As such, responsible plan fiduciaries should work proactively to mitigate potential risk.

Mitigating Risk Starts with Good Contracting

As the promotion of financial wellness offerings by recordkeepers and other service providers continues to expand, contractual terms around data usage are becoming more robust and complicated. The provisions are typically contained in two sets of terms: terms covering the use of participant data outside of core services and terms covering cybersecurity. Careful review, consideration and scrutiny should be paid to both sets of terms in order to protect the interests of participants and mitigate unnecessary fiduciary risk.

Terms Addressing Use of Participant Data

When entering into service agreements, responsible plan fiduciaries should be thinking critically about how they might reasonably make appropriate program offerings available without disregarding the fiduciary duties of loyalty and prudence. To strike a balance when negotiating service agreements, plan fiduciaries should consider the following:

- *Prohibit Unfettered Use of Data.* It is increasingly common for service agreements to provide for broad use of any data collected as an ERISA service provider. While these types of provisions arguably prevent the need for future service agreement updates, they may present unnecessary risk for fiduciaries and have significant potential for abuse. Good contract drafting necessitates defining the parameters for the use of participant data, the types of financial wellness offerings data will be applied to, how the plan fiduciaries will be kept informed of any changes in offerings and a mechanism by which the fiduciaries can restrict the offerings without terminating the ERISA service agreement. Such contractual terms help demonstrate fiduciary prudence by establishing clear boundaries and conditions for the use of participant data and ensuring that the core services offered are not beholden to continued commitment to ancillary offerings that will inevitably need to be reviewed as the landscape around use of participant data continues to evolve.
- *Prohibit the Sale of Data.* The sale of data collected by a service provider to third parties should be contractually prohibited. Data sales are not a financial wellness offering, result in additional (indirect) compensation to a service provider with speculative or no direct benefit to plan participants and result in the loss of control of such data.
- *Require Participants Consent to the Use of Data.* Individualized or targeted communications are undoubtedly an effective way to advertise financial wellness programs and help participants understand potential benefits of an offering, but a participant's data should not be used for such purposes without their consent. The reasons for this are twofold. First, a participant may not be interested in the product or offering and be frustrated that their data was used without their consent, resulting in complaints routinely directed to the Plan fiduciaries rather than the service provider. Second, unsolicited individualized communications are

more likely to lead a participant to incorrectly assume that the offering is part of an ERISA plan, and/or the offering has been endorsed by the plan fiduciaries. By requiring service providers obtain participant consent to any personalized use of their data—either during account registration, or through generalized correspondence asking interested participants to take action, participants will have better control over the use of their data and plan fiduciaries will be able to better prevent frustration and the illusion of tacit endorsement of offerings.

- *Avoid Fee Models Contingent Upon Use of Participant Data.* While financial wellness offerings may provide ancillary benefits to participants, they are also revenue generators for service providers. With that in mind, it is important that the use of participant data and marketing of financial wellness products not be tied to agreed-upon fees for services. This is relevant whether the sponsor or the participants bear the cost of services. Where the sponsor pays the service provider's fees and a portion of the fees are contingent upon the ability to market products and use participant data, a participant could claim that the plan sponsor allowed their data to be used to market products in order to save the sponsor money. Where the participants bear the service provider's fees, participants may raise claims regarding the reasonableness of the total compensation paid to the service provider, as well as the equitableness of fees based on varied usage of the additional services.
- *Avoid Substantive Terms of Wellness Programs in ERISA Plan Agreements.* A service agreement for an ERISA Plan should be prepared for the exclusive benefit of the participants and beneficiaries in that Plan; therefore, the terms of any ancillary program should not be spelled out in that agreement. This is important in not only satisfying ERISA's exclusive benefit rule, but also in avoiding an argument that the ancillary program is intended to be an ERISA plan, which if true would subject the plan fiduciaries to additional fiduciary responsibility and related liability.

Terms Addressing Cybersecurity

As technology evolves, including electronic communication, ERISA plans are growing targets for cyber attacks. While cybersecurity safeguards are critical in the maintenance of any ERISA plan, they have heightened importance where participant data may be used for ancillary purposes, as data is likely to be more robust, stored for longer and in more locations, and will necessarily be accessible by more parties. If participant data were to be accessed by unauthorized parties (a cybersecurity breach), it could compromise participant financial safety and security and expose the plan fiduciaries to liability.

In 2021, the Department of Labor (DOL) released cybersecurity best practices guidance (updated in 2024) [https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/compliance-assistance-releases/2024-01], which responsible plan fiduciaries should contractually require service providers (and their subsidiaries and affiliates) adhere to. Released in three pieces—one geared toward plan fiduciaries, one toward service providers, and one toward participants—the guidance underscores the importance of monitoring cybersecurity compliance as a fiduciary best practice. The DOL guidance should be treated as a minimum standard; to the extent a plan sponsor's business cybersecurity standards are greater than the standards established by the DOL, the plan sponsor should consider whether it would be appropriate to apply its business cybersecurity standards to agreements with ERISA plan service providers.

Importantly, plan fiduciaries should acknowledge the reality of cybersecurity breaches and be prepared to handle them when they arise. Fiduciaries should ensure both the plan and service providers have effective and ready-to-go breach remediation plans, such that appropriate actions can be taken as soon as reasonably

possible once a data breach is discovered. Equally important, fiduciaries should consider cybersecurity insurance and require service providers handling participant data to have cybersecurity insurance that covers any breach of participant data held by the service provider, its affiliates and subcontractors (if any).

Conclusion

While the *Williams-Linzey* case is in its infancy, the risks associated with maintenance and use of participant data are not new. Thoughtful consideration of the fiduciary issues discussed, which importantly include careful analysis of service provider contract terms can mitigate risk, permit reasonable financial wellness offerings and simultaneously protect plan participants.

If you have any questions about your recordkeeping contracts, financial wellness products, or use of participant data, contact the Trucker Huss attorneys with whom you usually work.

