



By **Deb Dupont**
Associate Managing Director, Worksite Retirement
LIMRA Secure Retirement Institute

Data and Security: A New Frontier

If data is the “new frontier” of customer engagement and experience, it’s a frontier that’s littered with potential land mines, especially in the financial services industry.

One landmine, participant data (and its many potential uses), has long been a subject of some contention between record keepers, advisors, and employers. (Whose clients/participants are they, anyway?) The recent Vanderbilt ruling is a potentially seismic event regarding how participant data is used, especially by record keepers.

Cybersecurity is another issue at the forefront of the industry’s collective consciousness. It creates an entirely new territory to be mapped in how we balance state-of-the-art messaging and engagement with protecting participants’ identities and information. The very nature of our business makes this absolutely imperative. While other industries may have a bit of a safety cushion, or room for a certain amount of error or mis-stepping with customer data, a breach the size of what we’ve seen elsewhere would likely prove fatal to a defined contribution (DC) record keeper.

At first read, the settlement in *Cassell vs. Vanderbilt* (a *settlement*, not a *court decision*) is an isolated event, in the 403(b) world of higher education plans. But an included term—that participant data *from the plan* not be used (by the plan’s record keeper or future record keepers) to “market” other products and services to participants, except when the participants have asked for the services—gives us pause. While currently limited to this settlement, potential for this restriction to be more broadly applied and interpreted as a fiduciary standard has set off alarms.

“Settlement in Vanderbilt 401(b) Case Raises Plan Data Questions,” states Groom Law.¹ “Cross-Selling is Poised to Be the Next 401(k) Battleground Issue,” says *Investment News*.² “Why 401(k) Advisors Should Be Concerned About the Latest Schlichter Settlement,” headlines *401(k) Specialist*.³ And, “Vanderbilt Settlement Sends Fiduciaries a Message,” proclaims *RetireAware*.⁴


Yes, this “settlement term” possibly has far-reaching implications. What are the “non-plan related” products and services that it vaguely identifies? How does this impact financial wellness services and programs that rely on personal data likely obtained in the course of offering a plan? What about new “sidecar” products such as education debt relief, emergency savings accounts, or HSAs? Outreach, adoption, and successful use of these products is intrinsically tied to personal situations and data. In a not-so-distant future, can a plan record keeper, or advisor, successfully include these products in their offerings without the context of participant data?

Protecting participant data, no matter how it may be used, is something of a “sacred trust” when we are facilitating retirement security.



Using participant data to offer more holistic suites of financial products and services, particularly under the umbrella of financial wellness, may be precluded by interpretations of the Vanderbilt settlement . . . but at what cost to participants for whom these offerings may offer a financial lifeline, or at least clear a path to successful savings? Our own research tells us that plan sponsors turn to record keepers to craft financial wellness programs and offerings. Denying the use of participant and plan data in these efforts may, at best, weaken the value propositions for participants—and, at worst, discourage the efforts from taking place entirely.

Data is a valuable commodity; therefore, so is the security of that commodity.



Participant data is essential to success for DC plan operations and outcomes for both sponsors and participants. Data is a valuable commodity; therefore, so is the security of that commodity.

Leventhal vs. Mandmarblestone Group LLC is a more recent suit, and it underscores the importance and critical nature of customer data from a different perspective: security. Here, a participant (Leventhal), after (presumably) properly making a TPA-facilitated withdrawal, evidently fell victim to a fraudster who withdrew the

remaining \$400k account balance, directing it to an alternate bank account. The suit is still in process, but a key learning—already—lies in the Court’s dismissal of two of the counts in the case (against the TPA and custodian), breach of contract and negligence . . . while ruling that a third count, *breach of fiduciary duty under ERISA*, could proceed.

When looked at together, these two scenarios highlight how different our industry is—and how much higher the stakes are—from many other businesses and platforms. We’re not Facebook, or Amazon, or even Experian. In the social, retail, and even some financial services sectors, data is used at will (or with very thin participant consent) to inform, market, and influence behavior, and not always to the consumer’s benefit. There’s a different bar for data protections and different accountability—and consequences—for breaches.

People use social media despite the well-documented and publicized data issues; they still use certain vendors, and shop at “compromised” stores. The data bar is set much higher for financial services and when people use DC plans. Our approach to data use overall—even as an everyday, standard capability—may be subject to additional restrictions and scrutiny. And it goes without saying that protecting participant data, no matter how it may be used, is something of a “sacred trust” when we are facilitating retirement security. 🌐

¹ “Settlement in Vanderbilt 401(B) Case Raises Plan Data Questions,” Groom Law, April 25, 2019, www.groom.com

² “Cross-Selling is Poised to be the next 401(k) battleground issue,” by Greg Iacurci, *Investment News*, May 12, 2019

³ “Why 401(k) Advisors Should Be Concerned About the Latest Schlichter Settlement,” by John Sullivan, 401(k) Specialist, August 26, 2019

⁴ “Vanderbilt Settlement Sends Fiduciaries a Message,” by Alan Steinberg, *RetireAware*, blog.retireaware.com