JOURNAL of PENSION BENEFITS

Issues in Administration, Design, Funding, and Compliance
Volume 30 • Number 2 • Winter 2023

401(k) Plans

Droning on about 401(k) Personal Data

A discussion of participant data and what needs to be protected and by whom.

By Michelle G. Murphy

Michelle G. Murphy, ERPA, QPA, QKC is Senior Manager and practice leader of Blue Benefits Consulting, Inc., a third-party administrator for qualified retirement plans. In addition to management and oversight of locations in Indiana and Ohio and a growing remote staff, she enjoys working with clients on effective plan design, and is responsible for business growth and sales. Mickie is a member of the American Society of Pension Professionals & Actuaries (ASPPA).

The fall color display in our area has been one of the most spectacular I have ever seen. I found myself wanting to document the colors of the leaves every day because they were changing fire red, orange, yellow, and different every time I stopped and looked. I wanted to save the photos for posterity so I could see this view again. Additionally, another thought that came to mind was that, when I get around to selling this house, I would love the buyers to know what kind of display they could have from the living room window. In discussing the color display phenomenon in a family gathering, the topic came up of drone photography and the ability to get spectacular views of a property that a photo from the ground cannot provide, especially if you have a few acres involved. We have all seen examples of what can be both beautiful and artistic with a view from above.

The talk then shifted to what else a drone can be used for, such as checking out the state of one's roof after a hailstorm instead of climbing a ladder up top, which quickly turned into jokes about dropping fireworks down a chimney if one were mischievous! As we went down the path from usefulness to mischief, the conversation also turned to invasion of privacy and having to keep the blinds closed in neighborhoods that permit residents to fly drones. Not only can drone

cameras have very powerful zoom lenses to capture what's on the ground, they can be aimed into open windows to capture photos, which is not just rude, but a type of invasion. No one wanted that kind of intrusion, even if it was harmless, so we close our blinds and draw the curtains to avoid it. Some people wish they could have a cloak of invisibility to protect them from being watched.

As an industry, are we going through the same thing with participant data?

There has never been a time in history where so much data is collected about individuals. When you sign into a webinar, your contact information is collected. Online shoppers are offered a discount if they provide their email address. We willingly give up information to participate in activities that we choose and most of us understand that we will receive emails and solicitations in return for sharing personal information. Sure, I will take that 20 percent discount and then stop the texts that I expect to follow!

In the retirement plan arena, more than an email address or cell phone is gathered to track participants and keep the plan in compliance with regulations. We are required to issue Forms 1099-R for distributions, as well as gather and report taxes. Many participants have the same name as others, so industry adopted the use of social security numbers as unique identifiers long before I was in the business. For eligibility, participation, and vesting purposes, we collect dates of birth, hire, termination, and death, which give us information needed to prepare those calculations but is also Protected Personal Information (PPI) for various legal purposes and which, if not properly protected, can be misused and lead to mischief. Cybersecurity webinars abound (I have notice of at least two in my inbox right now) because, as practitioners, third-party administrators (TPAs), recordkeepers, trustees, and advisors, we all have an obligation to protect our clients from bad players and fraud. None of us wants to see a participant's balance paid in error to someone who has obtained PPI, passwords, and other identifying information available in databases and social media through fraudulent acts. It is bad for participants, it is bad for business, and it can be expensive for practitioners, as well, if they are negligent and responsible for allowing a fraudster to get a foothold.

So, if we are diligent, we use the tools at hand to protect 401(k) participants, such as passwords that change aggravatingly often and multi-factor authentication for sign-ons. Many platforms no longer permit participants to change their address and request a distribution at the same time. Confirmation of address changes go to the current address to confirm, as well. We are protecting against the tricks that we are aware are used to identify as the participant and have funds sent to an account belonging to the fraudster. As an industry, we are doing the best we can to pull the shades, because we have discovered there is no cloak of invisibility.

While embezzling funds or stealing participant balances is criminal, not just mischievous, there are other concerns about participant data usage that does not fall into that category at all. What do we think about vendors using available data to send participants messages or information about products that might be of interest to them? Some years ago, I received a letter from my employer's insurance provider suggesting that, based on some pharmaceutical information that was available, I might be interested in certain medical information. They may have been right or they may have been off-target, but I was furious that someone had used my personal medical insurance data to suggest anything to me. It felt as an intrusion into information that was only shared between myself and my physician. It was explained to me that it was intended to help participants and to lower insurance costs, but the vendor took me off of the mailing list nonetheless.

Is there a similar trend starting with daily platforms where participants log in for balances and distribution modeling? The question can be raised regarding what data is stored when participants use modeling software and add information from outside assets to measure and predict goals and outcomes. Will the opportunity to purchase annuity investments or life insurance show up in an informational pop-up based on your age and spousal information? Who will be able to access the extra data that is not considered PPI? Will the recordkeeper own the data, or will the investment advisor have access to it? Will the TPA have access to the additional data, as well? Who gets to decide which data is private and which is not? (Legal counsel advises me that there have been court cases discussing to whom this data belongs—the plan, the participants, the employer? Is it a prohibited transaction for vendors to use this data to advertise their wares?)

I am concerned that the participant should be aware that anything that they provide on the website is available for additional use, even if just industry analysis. Retirement projections and modeling are

excellent tools for the plan participant to use for long-term planning and we want to encourage saving and planning in every way, but perhaps there should be a disclaimer posted that says data may be used for current or future statistical analysis purposes, or whatever the data will be used for.

Privacy is an almost universal concern these days. There are some people who might like to pull the blinds and close the curtains so the drone can't see all the way in. Perhaps those blinds and curtains belong in our computer systems, too. ■