

EBSA ERISA Advisory Council Meeting

October 18, 2022

This comment is submitted as a follow up to the Advisory Council Meeting of October 18, 2022, and the discussion of fiduciary duties surrounding cybersecurity and cybersecurity insurance.

1. Participant data and plan assets. It is difficult to see how the Labor Department can issue any guidance regarding fiduciary data protection duties without first confronting the elephant in the room – that is the question whether plan participant data is a “plan asset” under ERISA. This is one of the most significant issues of the day and the Department has failed to address the issue. The Department’s failure to act is not for want of encouragement. Our firm submitted an advisory opinion request in 2016 regarding the plan asset status of de-identified participant health plan data, but for reasons unknown, the Department has not responded to the request. In the meanwhile, the courts have weighed in on the status of identified 401(k) data, and the uniform conclusion to date is that the participant data is not a plan asset.

If participant data is a plan asset, the data would have to be held in trust, and anyone controlling or managing the data would be an ERISA fiduciary subject to the duties of prudence and loyalty, as well as the prohibited transaction rules. For plan recordkeepers, there would be a question whether their data access makes them functional ERISA fiduciaries or whether they are akin to a custodian with insufficient “control” or “management” over the data to be considered fiduciaries. If the recordkeeper is a fiduciary because of data control or management, the ERISA standard of care would apply to frame their duty to protect the plan asset.

If participant data is not a plan asset, an ERISA fiduciary presumably still has a duty to protect participant privacy based on a duty of confidentiality, which is rooted in the common law of trusts. Where a recordkeeper is not a fiduciary, however, plans are left with the difficult

contracting exercise of defining the recordkeeper's standard of care with respect to participant data protection. A number of legal academics have suggested that state law should be modified to recognize a new category of state law fiduciaries – “information fiduciaries” -- but that movement is in its infancy. In the meanwhile, plans must negotiate performance standards with recordkeepers, often landing on a “reasonable recordkeeper” standard, with little idea what such an industry standard really requires for data protection.

2. Indemnities and Insurance. A number of comments have said that plans should require plan vendors to provide cyber insurance and vendor indemnities to the plan to protect plan participants against cyber breaches. As a general matter, that seems quite appropriate and simple, but insurance and indemnities raise a host of other questions, based on who is insured and what is promised.

a. Insurance Coverage. Assume a 401(k) plan requires the recordkeeper to insure against cyber losses due to the recordkeeper's negligence. Assume also that the insurance covers all plan account losses, and also provides identity reconstruction services and participant credit monitoring in the event of a breach. Assume also that the recordkeeper fees were paid from plan assets.

If an event triggers collection under the insurance, what are the consequences? Are the account restoration payments treated as plan contributions, which means they are subject to dollar limits, or are they akin to investment earnings? The IRS ruling addressing 401(k) plan purchased disability insurance suggests they may be akin to earnings and not subject to dollar limits. *See PLR 200235043 (8/30/2002)*. Does it matter that the “highly compensated” employees had the largest plan balances—does the promised account restoration therefore involve a discriminatory right or feature under Code Section 401(a)(4)? And what is the status of the identity theft repair and credit monitoring payments? Would they be construed as plan

provided benefits that are disqualifying benefits or distributions? The IRS announced (Ann. 2015-22 and 2016-2) that identity theft benefits are considered tax-free benefits but that does not protect against a claim that they are disqualifying plan benefits.

The issues cannot be averted by having the plan procure insurance payable to the plan sponsor rather than to the plan. That would involve a clear violation of the exclusive benefit rule and it would involve prohibited transactions under ERISA Sections 406(a)(1)(D) and 406(b).

Some, but not all of, the concerns fall away if the recordkeeping agreement is between the plan sponsor and the recordkeeper, and plan assets are not used to procure the insurance. The plan sponsor could use the insurance proceeds to provide the identity theft and credit monitoring payments to the affected employees, but any insurance covering the account reconstitution would be problematic. The plan sponsor could not get the restoration payments back to the participant accounts to the extent that the payments are “contributions” subject to the IRS dollar limits and nondiscrimination testing. The IRS has provided leeway for certain “restorative” payments to plans by plan sponsors, but those are limited to cases where there was a reasonable basis for concluding that the plan sponsor had breached a fiduciary duty. That construct is not available in this case where it was the recordkeeper who was responsible for the cyber breach, and the recordkeeper is not an ERISA fiduciary. Another approach with a company-paid recordkeeping agreement might be to have the account restoration payments go directly to plan participants outside of the plan. Even if viewed as nontaxable because they are not an “accession to wealth” under classic tax doctrine, the restoration would not seem to be an eligible rollover and the fix would be imperfect.

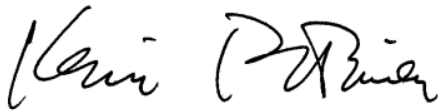
b. Vendor Indemnifications of Plans. Allowing recordkeepers and plan vendors to indemnify a plan is something that should be allowed, but it is something that also raises issues under current law. As one commentator already has noted, vendor indemnities

raise prohibited transaction concerns as possible extensions of credit based on prior Labor Department guidance. While it is highly unlikely that a fiduciary ever would face exposure for obtaining such indemnities, one concern is that a vendor might try and step away from the promised indemnity in the case of a widespread cyber event affecting thousands of participants. A case in point was *M&R Investment v. Fitz Simmons*, 484 F. Supp. 1041 (D. Nev. 1980), where the court refused to enforce a loan contract that involved a prohibited transaction. A plan always could argue that the recordkeeper indemnification is not a prohibited transaction based on a recent line of cases holding that ERISA Section 406(a) transactions are only “prohibited” if they involve a subjective intent to benefit the acting “party in interest”, which is not the case where the recordkeeper indemnity benefits the plan to the detriment of the recordkeeper. See *Sweda v. University of Pennsylvania*, 923 F.3d 320 (3d Cir. 2019). *Berkelhammer v. Automatic Data Processing, Inc.*, No. 20-5696 (ES) (JRA), 2022 WL 3593975 (D.N.J. August 23, 2022). But the Labor Department has not endorsed that argument and is probably unlikely to do so in light of long-standing guidance holding that Section 406(a) transactions are *per se* prohibitions. As the earlier comment pointed out, a sensible approach would be for the Labor Department to broaden the existing class exemption on interest free loans to allow vendor indemnities running to plan.

Even if the prohibited transaction question is addressed, vendor indemnities raise many of the same concerns outlined above with insurance. Some indemnities promise to cover both direct as well as consequential participant damages. Participant consequential damages attributed to a cyber breach could cover all kinds of losses – from bank accounts to credit card usage. If the indemnity runs to the 401(k) plan, what does it do with the recovery? How does the plan get it back to the affected participants? These may seem like nit-picky details, but it all has to be worked out to make it all work smoothly. As with the insurance case, the issues cannot be avoided by having the indemnification payments made to the plan sponsor or the

plan participant rather than the plan—there are exclusive benefit concerns, plan qualification and impracticability concerns.

Cyber security insurance and indemnification is not as simple as many have imagined and various issues need to be addressed up-front before any fiduciary “best practice” can be endorsed. The Labor Department cannot act alone in this effort and should coordinate where appropriate with the Internal Revenue Service. At the same time the degree of difficulty of some of these issues is not a reason to dither; the consequences are too important – both for participants and for employers and plan fiduciaries seeking to ensure compliance. The Labor Department should not wait to see how these questions play out in the marketplace and in the courts and should instead address them as soon as possible.



Kevin P. O'Brien
Ivins, Phillips & Barker
1717 K Street NW, Suite 600
Washington DC 20006
202-662-3411