Recalibrating Employee Benefits and Compensation Strategies
A HUB International Series

Responding to Employee Retirement Plan Liability Risks

HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

RECALIBRATING EMPLOYEE RETIREMENT BENEFITS

Responding to Employee Retirement Plan Liability Risks

The global pandemic, along with the changing economic and social landscape impacts employee benefits programs in many ways. The pressure to manage costs and compliance while supporting employees has never been greater.

In this eBook, HUB International explores how the COVID-19 pandemic has amplified fiduciary risks for employee retirement plan sponsors and committees. It covers three key risks and provides guidance on how to mitigate these risks and avoid costly litigation.

Explore our entire eBook series on ***Recalibrating Employee Benefits and Compensation Strategies*** so you can be well-positioned to meet tomorrow's challenges:

1. Enhancing Health Plan Financial Stability and Employee Engagement
   ▸ READ MORE
2. Responding to Employee Retirement Plan Liability Risks
3. Building a Meaningful Compensation Strategy for Today's Workforce
   ▸ READ MORE

Risk #1: ERISA Litigation — The Biggest Risk for Fiduciaries

In a year marked by one extraordinary event after another, here's another for the books: the pace of lawsuits filed over 401(k) fees jumped dramatically in 2020 over 2019 levels. In the first eight months of the year, more than 60 such cases were filed. In 2019, there were 20.

And another worrisome development: some employers have even been sued twice in 2020[1] over plans that some participants claimed are too expensive. After 2019, when ERISA class settlements reached $449 million[2], there's cause for concern among plan sponsors and their committees that serve as primary fiduciaries. For all the time they spend on the quality of investments in their plans, the bigger bone of contention is costs – of recordkeepers and of investments.

Here's what's important to know about these claims and steps that can help minimize the fiduciary risks.

Recordkeeper fees: Make indirect compensation more transparent

Typically, a plan's recordkeeper is paid by charges to the plan and participants' accounts – "direct" compensation – and by revenue it receives from the plan's investments – "indirect" compensation. Both must be considered when evaluating whether the recordkeeper's fees are reasonable and fair. While plan fiduciaries can easily observe the direct payments, indirect compensation is difficult to understand, for two reasons. The first is terminology; payments might be called revenue sharing, administrative fees, or 12b-1 fees, among others. Second, the payments are made by the investment managers (or other service providers) without being reported to the committee.

Strategic Tip: Plan sponsors should make a practice of benchmarking recordkeeper's fees regularly – every three years is a good rule of thumb. Benchmarking services enable plan sponsors and advisers to compare costs and compensation by providing information about the direct and indirect compensation paid by "peer" plans.

[1] *https://news.bloomberglaw.com/employee-benefits/401k-fee-suits-flood-courts-on-pace-for-fivefold-jump-in-2020*

[2] *https://news.bloomberglaw.com/employee-benefits/erisa-class-settlements-rebounded-to-449-million-in-2019*

(A peer plan is comparable by virtue of similar total assets and numbers of participants, the primary factors in recordkeeper compensation.) Benchmarking reports combined with the guidance of an experienced plan adviser, will show committee members how their plan payments stack up.

A precautionary note: Average compensation does not, in and of itself, determine reasonableness. The objective is to fall within the range of reasonable fees. Plus, the quality and quantity of services received by the plan and the participants should also influence the assessment. Your HUB retirement specialist can help you gauge if higher pay is merited.

Plan sponsors might also opt to go through a Request for Proposal process to get similar fee comparisons. This can be burdensome and expensive, which is why benchmarking is more often used.

Investment expenses: A complicated assessment

Investment expenses also should be evaluated based on industry averages. Most plan advisors can readily supply reports of expenses for different types of investments and help make sure that a reasonable amount is being paid.

But there's more to it than that. As plan assets increase, lower cost "share classes" of a mutual fund become available to the plan. A mutual fund may have several share classes, all of which are invested in the same pool of investments. But each share class has a different expense ratio. Larger plans can invest in the cheaper share classes. A safe approach is for a plan to invest in the lowest cost share class available to it. This is complicated. Mutual funds typically have stated minimums for lower cost share classes. But some funds will, if asked, waive that requirement for retirement plans.

Another complication is that some share classes may pay revenue sharing to the plan. When the revenue sharing is subtracted from the expense ratio for that share class, it can be less expensive than a share class that appears to be cheaper. It's another front where an experienced retirement plan adviser is invaluable.

Strategic Tip: The reality is that some of the issues facing plan committees are outside their typical member's experience and knowledge. The law says that in their capacity as fiduciaries, committee members are not required to have that knowledge. Instead, they can hire professionals, such as advisers and attorneys, to help them make prudent decisions. As ERISA litigation steps up, this is one area where they have a critical role to play.

Risk #2: Mining Employee Data to Guide Financial Wellness Programs

It's increasingly common for 401(k) recordkeepers and some advisers to offer financial wellness programs for plan participants, typically using participant and employee data to customize their advice and educational services. It's a logical approach but recent lawsuits challenge the use of participant data.

Financial wellness programs can incorporate a wide array of services to help employees deal with increasingly complex financial issues. The trend responds to the high level of financial stress in the U.S. workforce – so problematic that as many as 83% of employers with over 100 employees have instituted programs to help.[3]

Retirement plan participants may be offered advice on salary deferment practices and tradeoffs, managing student debt, and contributing to Health Savings Accounts. Guidance offered can have a long-term financial impact on a participant; it can be customized when provided by the plan's recordkeeper, which has "participant data" for plan administration purposes. Using the data, which also can be shared with the adviser for financial wellness advice, makes for better quality guidance.

This didn't present a fiduciary problem until plaintiffs' class action law firms began including a claim of fiduciary breach in its lawsuits against plan sponsors and committees. The lawsuits mainly claim the fiduciary fault in managing investment and recordkeeper expenses. A claim over use of participant data is an add-on.

Only one such case has been decided, and in favor of the plan sponsor, Northwestern University. But the issue continues to be litigated in other cases.

[3] *https://www.pionline.com/article/20180903/PRINT/180909977/gauging-value-of-financial-wellness-plans-a-struggle*

Strategic Tip: start by understanding the plaintiffs' attorney claims. Plan sponsors and committees should be aware of the issue, find out if their service providers are using participant data to offer financial wellness programs, and decide if these should be offered to their plan's participants.

Claim #1
Service providers use the participant data to sell expensive services and investments to the participants.

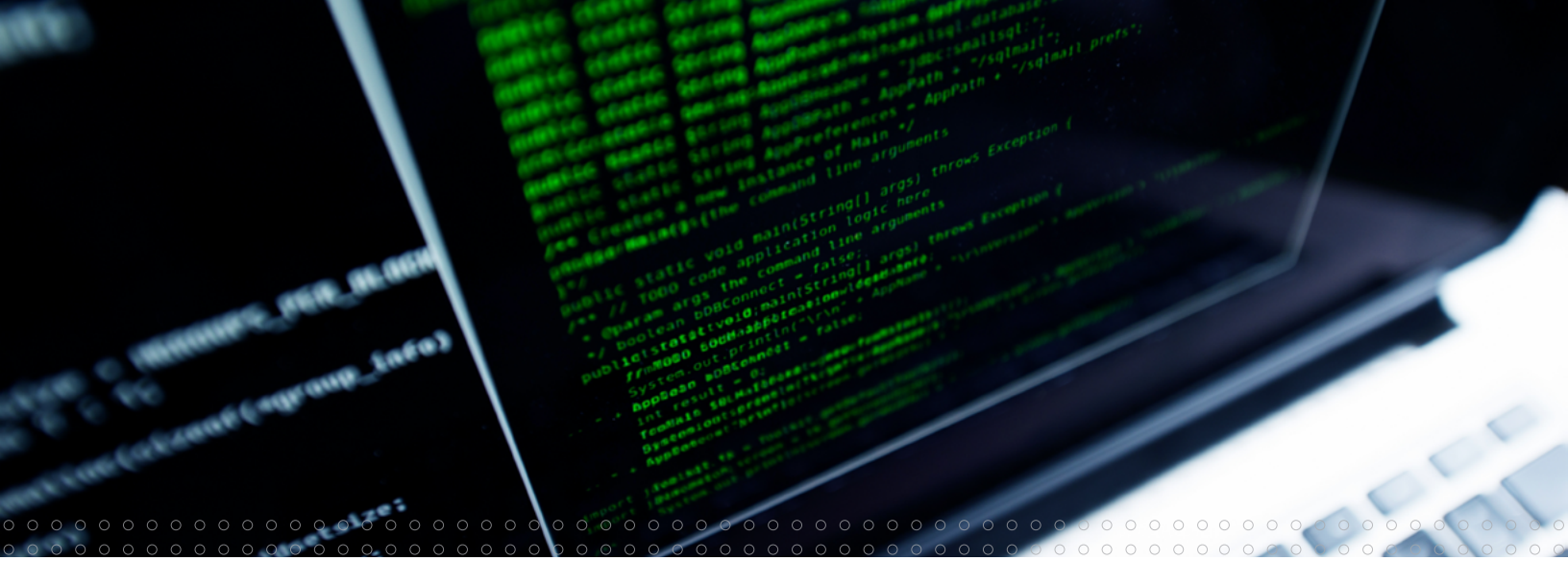
The claim isn't necessarily true, but plan committees can protect themselves by having their service providers explain the financial wellness services being provided and their quality and costs. This should include how conflicts of interest are disclosed and managed. Then, the committee, with the plan's adviser and attorney, should determine whether the services are valuable to the participants, quality and costs are reasonable, and conflicts are properly managed. The recordkeeping or advisory agreement should be reviewed and aligned with the committee's review and decision.

Plaintiffs' attorneys argue that participant data should not be used unless a participant affirmatively says that it can. But that's not the law. (Such a provision has been included in voluntary settlements – but those have not been part of a court decision.) ERISA requires a prudent decision-making process by fiduciaries. If a committee reasonably concludes that financial wellness services are helpful to their participants and engages in an informed and reasoned process to evaluate and approve the services and costs, the "prudent man" rule will have been satisfied.

Claim #2
If service providers make money from participant services, profits from that revenue should be factored into the service provider's fees.

To avoid that claim, committees should, with help from their plan advisers, determine whether the cost of the recordkeeper's services are reasonable, taking into account all revenues being received related to plan and participant services.

The use of participant data is an emerging issue for plan sponsors and committees. Since the fiduciary rules in this area are not clearly defined, the best course for plan committees is to thoughtfully weigh the quality and value of the financial wellness programs being offered to plan participants.



Risk #3: Cyber Thieves & Participant Accounts: A Fiduciary Responsibility?

Three lawsuits over the theft by cyber criminals from the investment accounts of retirement plan participants shine a spotlight on fiduciary responsibility and how far it goes. There is little official guidance on the matter of cyber thieves, but the lawsuits are increasing the risk for employers. As a result, plan sponsors and fiduciaries should consider taking steps to minimize that risk.

Cyber theft has skyrocketed during the pandemic. By June 2020, the daily digital crime rate was 74% ahead of where it was when stay-at-home restrictions were put in place.[4] A lucrative target? The investment accounts of retirement plan participants. Why? The risk has escalated with remote work combined with increased distribution and loan limits under the CARES Act.

Plan sponsors are right to be uneasy over their potential fiduciary responsibility to prevent these crimes, and understandably. There's little guidance from the Department of Labor or definitive answers from recent related court decisions.

But employers can gain insights from three pending cases brought by plan participants.

[4] https://www.ic3.gov/

Lawsuit #1:
Service partners' practices matter

THE CASE: In *Barnett v. Abbott Laboratories*, a cyber thief obtained a 401(k) account login information, except for the password, logged into the account at the recordkeeper, and clicked on the "Forgot Password" button. The thief intercepted the email with the new password, changed the bank account of record for disbursements and had $245,000 from the retired participant's account transferred to the new bank. The plaintiff complained that if the plan's recordkeeper had notified her of the requested withdrawal via email (apparently her preferred method of communication), rather than a letter, it would have been timely enough to stop the transfer.

THE FINDINGS: The court held that the plan sponsor was not liable, but the recordkeeper could be. That ruling may not give plan sponsors much comfort, though, an argument could be made that in their capacity as fiduciaries (usually through plan committees), they have a duty to investigate and monitor the cyber security procedures of their service providers.

LESSONS LEARNED: With the law here unsettled, a cautious approach begins with plan sponsors acquainting themselves with the cyber security policies and procedures of their service providers, particularly the plan's recordkeeper. Internal IT staff or consultants should evaluate those procedures against industry standards. Plan advisors can explain best practices in the 401(k) industry. Service providers should explain how they monitor compliance. Finally, ask for an update on those procedures regularly. On a different front, the plan's lawyer should review its service provider agreements, advising on provisions for both sides' cyber security responsibilities and any limitations on the service providers' liability.

Lawsuit #2:
When service providers countersue

THE CASE: In *Leventhal v. MandMarblestone Group* a cyber thief stole $400,000 from a participant's account by intercepting emails from an employee who was working remotely. The plan's service providers were sued.

THE FINDINGS: In a procedural motion, the court found that the service providers could be liable as fiduciaries. But they countersued the plan sponsor, arguing that its responsibilities were breached in allowing remote work without proper cyber security safeguards. The court decided that the counterclaim was sufficient to proceed to trial, leaving open the possibility that the plan sponsor would be at least partially liable.

LESSONS LEARNED: This court found that plan sponsors and committees could be responsible to have reasonable procedures in place to protect communications of employees about the retirement plans and distributions. This is a particularly acute issue given the prevalence of remote working during the pandemic. Plan sponsors should enlist their IT people in developing security practices that ideally exceed standard practices. It's better to avoid a loss than to defend against it.

Lawsuit #3:
Avoiding shared failures in account security

THE CASE: In *Berman v. Estee Lauder, Inc.* a cyber thief stole almost $90,000 from a participant's account, apparently by obtaining the participant's login information, changing the bank account, and making withdrawals. The participant sued, alleging that the plan sponsor, recordkeeper and trustee all breached their fiduciary duties. The case was subsequently settled.

LESSONS LEARNED: Few details about the case are known, but some takeaways are available. First, since cyber thieves sometimes obtain partial or complete login information from plan participants, it's important to provide the participants with ongoing education about protecting their login information and passwords. Second, committees should review their service providers' procedures for protecting accounts. When bank accounts are changed, a red flag goes up that a participant's money could be in jeopardy. Are there dual authentication procedures for a withdrawal…perhaps a text after the initial login and request? The same question should be asked about changes of passwords, which is a common practice of cyber thieves.

The views expressed in this article are those of Fred Reish, and not necessarily of Faegre Drinker. The article is for general information only and is not intended to provide investment, tax or legal advice, or recommendations for any particular situation. Please consult with a financial, tax or legal advisor on your circumstances.

HUB International's retirement plan fiduciary advisors provide ongoing guidance on your plan's setup and management to ensure it meets regulatory compliance guidelines and the interests of your employees. Contact HUB to request an assessment of your group retirement plan.

Fred Reish is a partner with the law firm of Faegre Drinker who specializes in retirement law, focusing on fiduciary and best interest standards of care, prohibited transactions, conflicts of interest, and retirement plans.

Strategic support that puts you in control.

Whether you want to promote better outcomes for your retirement plan participants or pursue your individual financial goals, we can help. HUB Retirement and Private Wealth offers knowledgeable specialists who will tailor strategies to address your specific needs. As investment fiduciaries, we work solely on your behalf and are committed to your success.

Hubretirementplans.com

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

HUB