ERISA Roundup

A quarterly recap of recent publications from BDO's ERISA Center of Excellence

Q3 2023

A NOTE FROM BDO'S NATIONAL ERISA PRACTICE LEADER

As the leaves have changed colors and we are well into Fall, it is the perfect time to take stock of those retirement plan-related tasks that you may have been putting off during the plan audit and Form 5500 filing rush.

In this edition of our ERISA Roundup, we explore the importance of clear communications during open enrollment and monitoring employee deferral limits before the end of the year. We dive into cybersecurity impacts on retirement plans, as well as explore more of the key priorities of SECURE Act 2.0.

Staying current on ERISA topics is simplified with BDO as we invite you to follow along with our regular insights at our **BDO ERISA Center of Excellence** and our podcast series **BDO Talks ERISA**. We welcome any feedback on our content at **BDOTalksERISA@BDO.com**.

Best,

BETH GARNER
National Practice Leader,
EBP and ERISA Services

IN THIS ISSUE

BDO's ERISA Center of Excellence is your source for insights on emerging regulations, industry trends, current topics, and more. Visit us at **www.bdo.com/erisa** or follow along on Twitter: @BDO_USA and #BDOERISA.

2023 Deadlines and Important Dates

Sponsors of defined benefit and defined contribution retirement plans should keep the following deadlines and other important dates in mind as they work toward ensuring compliance for their plans in 2023. Dates assume a calendar year plan. Some deadlines may not apply, or dates may shift based on the plan sponsor's fiscal year. For additional support, please contact your BDO representative.

OCTOBER

- **1** / **Action:** Distribute annual notices to participants no earlier than October 1 and no later than Dec 1, including notices for: 401(k) Plan Safe Harbor Match, Automatic Contribution Arrangement Safe Harbor, Automatic Enrollment and Qualified Default Investment Alternatives (QDIA).
- **13** / **Fund:** October 13 possible third quarter 2022 contribution due for defined benefit pension plans.
- **16** / **Action:** October 16 is the extended deadline for filing IRS Form 5500 and IRS Form 8955-SSA.
- **16** / **Action:** October 16 is the extended deadline for filing individual and C-Corp tax returns.
- **16** / **Action:** If an extension was filed, October 16 is the deadline to fund defined contribution employer contributions for C-Corporations and Sole Proprietors.
- **16** / **Action:** October 16 to open a Simplified Employee Pension (SEP) plan for extended tax filers.
- **16** / **Action:** Send annual funding notice to participants of single- and multi-employer defined benefit plans with 100 or fewer participants by October 16.
- **16** / **Action:** File PBGC Form 10, Post-Event Notice of Reportable Events, by October 16, if a defined benefit plan (of any size) missed its September 15 required contribution. A filing is not due if a PBGC Form 200 was already filed for the same event.
- **16** / **Action:** October 16, defined benefit plan PBGC Premium filings and payments due.
- **25** / **Action:** File PBGC Form 200, Notice of Failure to Make Required Contributions, by October 25, if plan sponsor of a single-employer defined benefit plan does not make the October 15 required contribution, causing the plan to have more than $1 million in unpaid contributions.
- **30** / **Action:** Single-employer defined benefit plans that are less than 60% funded or are 80% funded and have benefit restrictions triggered must inform participants by October 30 or 30 days after the benefit restriction applies.

Best Practice: Make sure administrative procedures align with language in plan document.

NOVEMBER

- **15** / **Action:** File PBGC Form 10, Post-Event Notice of Reportable Events, by November 15, if a defined benefit plan with 100 participants missed its October 15 required contribution and it remains uncontributed. Filing is not required if the contribution could have been met with a Prefunding or Carryover Balance election or if a PBGC Form 200, Notice of Failure to Make Required Contributions, was already filed for the same event.

Best Practice: Plans may consider doing mid-year compliance testing to avoid failing applicable annual tests.

DECEMBER

- **1** / **Action:** Distribute annual participant notices no later than December 1. These include notices for: 401(k) Plan Safe Harbor Match, Automatic Contribution Arrangement Safe Harbor, Automatic Enrollment and Qualified Default Investment Alternatives (QDIA).
- **15** / **Action:** December 15 is the extended deadline to distribute Summary Annual Report (SAR) when the Form 5500 was filed on October 16.
- **29** / **Action:** December 29 is the final deadline to process corrective distributions for failed ADP/ACP testing; a 10% excise tax may apply.
- **29** / **Action:** Ongoing required minimum distributions (RMDs) for 5% business owners and terminated participants must be completed by December 29.
- **31** / **Action:** Amendments to change traditional 401(k) to safe harbor design, remove safe harbor feature or change certain discretionary modifications must be completed by December 31. Amendments to change to safe harbor nonelective design must be completed by Dec 1 of given plan year for 3% or by Dec 31 of the following year for 4% contribution level.
- **31** / **Action:** Plan sponsors must amend plan documents by December 31 for any discretionary changes made during the year.

Retirement Plans & Cybersecurity: Insights for Plan Sponsors

Cybersecurity is a top concern for many U.S. businesses and industries. The retirement plan industry holds over $37 trillion in total participant retirement accounts, yet only 27 percent of plan sponsors have a written cybersecurity policy, according to the 65th annual S**urvey of Profit Sharing and 401(k) Plans** by the Plan Sponsor Council of America (PSCA). Government regulation has driven cybersecurity enhancements in other industries (such as enhanced safeguards for credit cards and online accounts in the banking industry). While the retirement industry currently lacks a comprehensive system of cybersecurity laws and regulations, the Department of Labor (DOL) has turned its attention to cybersecurity for employee benefit plans.

DEPARTMENT OF LABOR (DOL) CYBERSECURITY TWO-PRONGED FOCUS

In April 2021, the DOL issued cybersecurity **guidance** or tips for plan sponsors when hiring a **service provider**, best **protection practices**, and **online security information** for participants and beneficiaries. None of this guidance is required by law, but the DOL is using these tools as a basis to ask for more cybersecurity-related information when it conducts audits plans. Since issuing the guidelines, the DOL has increasingly expressed interest in gathering information about audited plans' documents for policies, procedures, and guidelines related to cybersecurity. It has also begun requesting specific details from plan sponsors as to how their plan service providers use participant data. According to the PSCA study, 56 percent of plans have a participant data use policy as part of the recordkeeper service agreement. If a plan is audited by the DOL, the plan sponsor should be prepared to answer questions about such policies and provide follow-up information if requested.

ERISA ADVISORY COUNCIL'S REPORT ON CYBERSECURITY INSURANCE

The DOL **ERISA Advisory Council** (the Council) consists of 15 appointees representing interests of employer organizations, employers, specific industry fields, and the general public. The Council's December 2022 **report** analyzed how cybersecurity insurance addresses risk in employee benefit plans. The council heard from a number of industry experts representing a wide cross-section of interests — central themes of the testimonies shared were that the issue is complex, not widely understood, and requires further study. For instance, one witness suggested the Council consider whether the Employee Retirement Income Security Act of 1974 (ERISA) requires plan fiduciaries and service providers to guarantee a loss when they took reasonable steps to prevent fraud.

WHAT CAN PLAN SPONSORS DO TO MITIGATE CYBER RISKS

With the increased regulatory focus and greater awareness of cyber vulnerabilities within the retirement plan industry, plan sponsors are looking for ways to meet their fiduciary responsibility in mitigating retirement plan cybersecurity risks. The following are just a few of the currently available ways in which sponsors can address the risks:

- **Cybersecurity Insurance:** For sponsors considering retirement plan cybersecurity insurance, a key question when evaluating potential policies is asking which party would be liable for a cybersecurity breach. Additional considerations include identifying who is the insured party (the sponsor, the plan or both?), who is responsible for purchasing the policy (the sponsor or the plan?), and the full scope of the policy (in other words, what is or is not covered in the event of a cyber breach?).

  Another aspect to think about is how much coverage is needed for the policy. According to this year's **IBM Cost of Data Breach Report** the average cost of a breach in the United States was $9.48 million. The sponsor should also consider factors unique to its company and the plan, etc.

- **Cybersecurity Risk Management Program:** Through the DOL's audit investigations, some sponsors are feeling increased pressure to implement a cybersecurity risk management program that has policies and procedures directly addressing the employee benefit plan.

  If a sponsor decides to adopt a risk management program, ensuring the policy is the right fit is crucial. A boiler-plate policy is generally not a good approach since it may not fully align with the company's processes and procedures. Any program put in place around the plan's cybersecurity should be clearly understood, routinely followed and updated regularly. A program that is put into place, but not followed or updated could become substantiating evidence in the event of plan litigation following a cyber breach.

- **Add IT to the Plan Committee:** With the ever-evolving cyber technology, adding an IT professional to the plan administrative committee (those charged with plan governance) informs the committee about emerging trends and advancements in cybersecurity. The IT professional can also help educate on the latest cyber tools and best practices, as well help in the evaluation process to understand the technological aspects of the plan, such as software systems, data security, and infrastructure requirement. This professional can also encourage the committee to provide appropriate time and resources for plan cybersecurity.

  Overall, inclusion of an IT proficient employee on the committee charged with oversight and administration of the plan can help ensure the technology-related aspects of the retirement plan are well-managed, secure, and aligned with the company's goals.

- **Cybersecurity Is a Shared Responsibility:** The cyber community has fully embraced that it is no longer a question of who is responsible in the event of a cyber breach, but rather that all parties share in the responsibility for cybersecurity. The plan sponsor can play a key role in educating plan participants about their role in building a stronger cybersecurity defense. This education would include emerging trends in cyberhacking and proper risk-mitigation practices, such as two-factor authentication, regular account monitoring and avoidance of phishing attacks. The PSCA study reported 61% of plans have cybersecurity awareness campaigns and half have issued email alerts on specific cyber issues.

BDO INSIGHT: Pay Attention to the Plan's Cybersecurity Process

When determining a comprehensive approach to cybersecurity and assessing the plan's cyber risk profile, plan sponsors should remember that ERISA's standard of care stipulates fiduciaries must act in the best interests of participants and beneficiaries. Cybersecurity risks are an ongoing part of current-day plan administration — as such, plan fiduciaries have a responsibility to ask questions and take procedural steps to lessen cybersecurity risk is as much as reasonably possible.

Knowing what the plan's service providers are doing to prevent cybersecurity attacks, educating participants, and documenting policies and controls are all sound actions to protect both the plan and the sponsor in the event of a cyber-breach.

For larger plan sponsors or those who have experienced a breach, System and Organization Controls (SOC) for cybersecurity reports can provide an independent assessment of the sponsor's implemented cybersecurity controls. Having these reports allows plan sponsors to better manage their risk, support compliance, promote transparency, and make informed decisions about plan vendor selection and monitoring.

Each plan sponsor is tasked with evaluating their plan's unique cybersecurity risks and needs. Your BDO representative can help you assess your plan's current cyber risk profile.

2024 Cost-of-Living Adjustments for Qualified Retirement Plans

BDO presents a highlights summary of the significant cost-of-living adjustments (COLA) effective for 2024. These adjustments recently announced by the Internal Revenue Service (IRS) and the Social Security Administration (SSA) have a wide-ranging impact, including the savings rate for retirement plans. In general, annual compensation amounts and limits for elective deferrals were increased, while catch-up contribution limits remain unchanged. BDO will continue to provide updates on regulatory matters impacting retirement plans in the coming year – to sign up for BDO newsletters and other insights, visit the **ERISA Center of Excellence**.

Code Section	2024	2023	2022
401(a)(17) /404(l) Annual Compensation	$345,000	$330,000	$305,000
402(g)(1) Elective Deferrals	$23,000	$22,500	$20,500
408(k)(2)(C) SEP Minimum Compensation	$750	$750	$650
408(k)(3)(C) SEP Maximum Compensation	$345,000	$330,000	$305,000
408(p)(2)(E) SIMPLE Maximum Contributions	$16,000	$15,500	$14,000
409(o)(1)(C)(ii) ESOP Limits	$1,380,000 $275,000	$1,330,000 $265,000	$123,000 $245,000
414(q)(1)(B) HCE Threshold	$155,000	$150,000	$135,000
414(v)(2)(B)(i) Catch-up Contributions	$7,500	$7,500	$6,500
414(v)(2)(B)(ii) Catch-up Contributions	$3,500	$3,500	$3,000
415(b)(1)(A) DB Limits	$275,000	$265,000	$245,000
415(c)(1)(A) DC Limits	$69,000	$66,000	$61,000
416(i)(1)(A)(i) Key Employee	$220,000	$215,000	$200,000
457(e)(15) Deferral Limits	$23,000	$22,500	$20,500
1.61-21(f)(5)(i) Control Employee	$135,000	$130,000	$120,000
1.61-21(f)(5)(iii) Control Employee	$275,000	$265,000	$245,000
Taxable Wage Base for Social Security	$168,600	$160,200	$147,000

BDO works collaboratively with clients to test retirement plan limits while performing an audit of the qualified retirement plan. For more information about our ERISA audit services, plan administration and actuarial services, visit BDO's **Employee Benefit Plan Audits**.

Clarifying the SECURE Act 2.0 Roth Catch-Up Contribution Extension

While, the IRS' announcement last month provides significant compliance relief for processing catch-up contributions as after-tax "Roth" contributions, the focus now for plan sponsors should be on proper implementation of the guidance. IRS **Notice 2023-62** established a two-year administrative extension window for plan sponsors to delay their implementation of mandated changes required by the SECURE 2.0 Act of 2022 until January 1, 2026. It also clarified that the IRS will allow catch-up contributions to continue to be made under pre-SECURE 2.0 law for plan years starting in 2024.

The IRS took this action to address a drafting mistake in **Section 603** of SECURE 2.0 that technically eliminated all catch-up contributions by accidentally deleting IRC Section 402(g)(1)(C). Legislators have indicated Congress intends to resolve this error with a future technical correction.

This extension was welcomed by the defined contribution retirement plan community, which had previously voiced concerns about having insufficient time to update their systems to implement the provision. Section 603 of SECURE 2.0 had originally required catch-up contributions made to a qualified retirement plan — such as 401(k), 403(b), or 457(b) plans — by higher income employees (who earned $145,000 or more in the prior year) to be made on a Roth basis beginning January 1, 2024. Despite the recent extension, additional clarification is needed for plan administrators, sponsors, and other key stakeholders to fully understand their regulatory burden.

EXECUTION CHALLENGES

The new so-called "Rothification" rules had generated numerous questions from key retirement plan industry stakeholders, including large employers. There were also requests for additional implementation time as well as for more detailed and clarifying regulatory guidance. For instance, the ERISA Industry Committee (ERIC) published an **open letter** in July 2023 that cited a number of administrative hurdles for implementation and the need for transition relief.

One concern cited was the new $145,000 income limit imposed on Roth catch-up contributions. Because it is a brand-new threshold (and not part of any existing qualified plan rule or requirement), implementation would require plan sponsors to coordinate closely with their payroll administrators, recordkeepers, and other service providers to make the necessary system updates. The new income limit is also anticipated to have a significant trickle-down impact on both sponsor and provider systems and processes.

Plan sponsors also need to develop and roll out communication of the changes to employees, which requires IRS guidance that had not yet been provided. As ERIC's open letter indicated, the industry had concerns that starting implementation before the issuance of IRS guidance could result in costly re-work. Additionally, employers whose plans do not currently allow for Roth plan contributions faced a dilemma as to whether to eliminate catch-up contributions entirely (at least, until they were able to implement a Roth program) or attempt to quickly implement a Roth option.

WELCOME RELIEF

The IRS notice provides a two-year administrative transition period during which qualified retirement plans offering catch-up contributions will be treated as satisfying the new rules in Section 414(v)(7)(A) even if the contributions are not designated as Roth contributions throughout the transition period (or until December 31, 2025). Additionally, a plan that does not currently provide for any designated Roth contributions will still be treated as satisfying the new requirements.

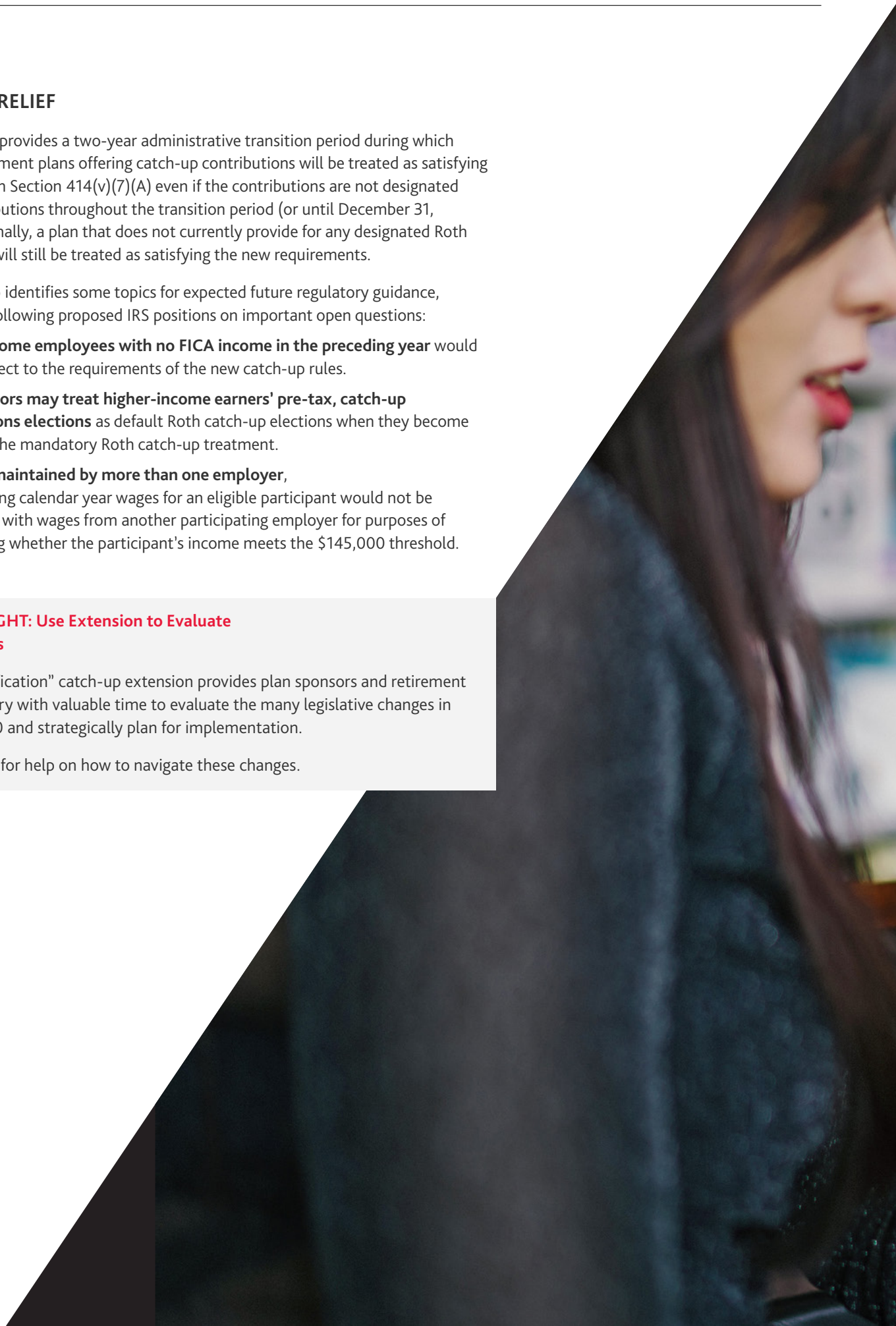
The notice also identifies some topics for expected future regulatory guidance, including the following proposed IRS positions on important open questions:

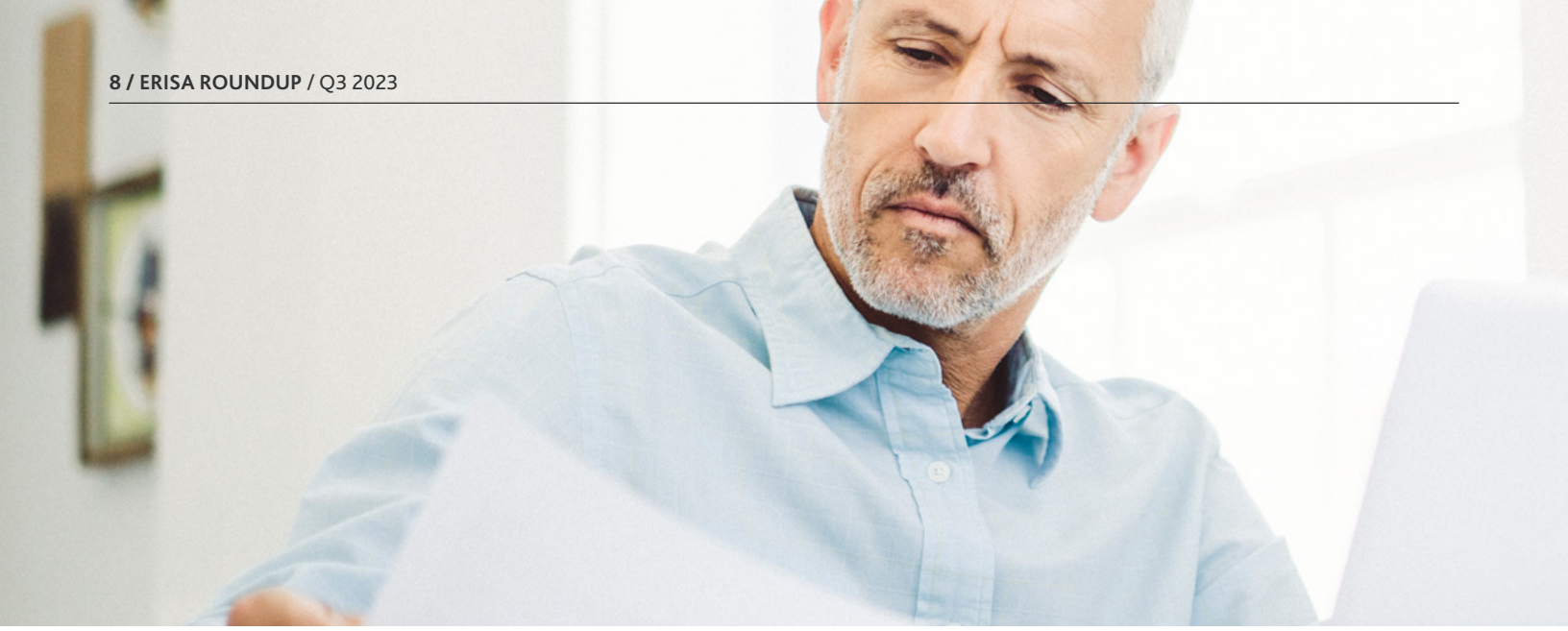
- **Higher-income employees with no FICA income in the preceding year** would not be subject to the requirements of the new catch-up rules.
- **Plan sponsors may treat higher-income earners' pre-tax, catch-up contributions elections** as default Roth catch-up elections when they become subject to the mandatory Roth catch-up treatment.
- **For plans maintained by more than one employer**, the preceding calendar year wages for an eligible participant would not be aggregated with wages from another participating employer for purposes of determining whether the participant's income meets the $145,000 threshold.

BDO INSIGHT: Use Extension to Evaluate Next Steps

The "Rothification" catch-up extension provides plan sponsors and retirement plan industry with valuable time to evaluate the many legislative changes in SECURE 2.0 and strategically plan for implementation.

Contact us for help on how to navigate these changes.





Safeguarding Retirement Savings: Inside Secure Act 2.0 Key Priorities

Most of the 90-plus provisions included in the SECURE 2.0 Act of 2022 ("Secure 2.0", "the Act") are aimed at preserving and enhancing the retirement savings of working Americans and improving the effectiveness of retirement plan administration for plan sponsors.

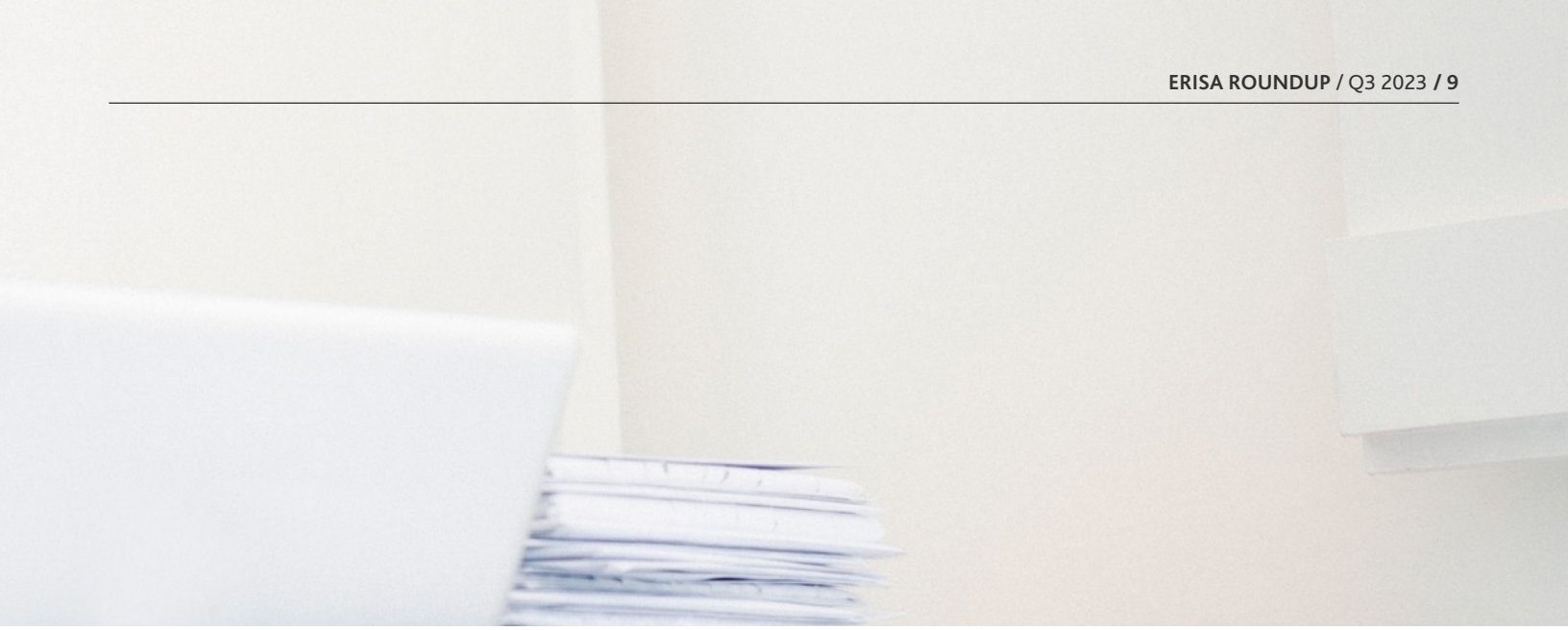
A key priority of the Act is to strengthen retirement savings by keeping employees connected to their retirement accounts as they move from job to job while also reducing leakage of retirement savings out of ERISA plans. The Act stipulates the creation of a lost and found database to assist retirement plan participants in locating retirement accounts from former employers. The Act seeks to streamline the movement of retirement benefits to reduce either misplaced monies or prematurely distributed funds, which is referred to as automatic portability. In keeping with this goal, a provision of the Act mandates development of a system that automatically rolls over retirement savings to a new plan when employees change jobs (essentially tethering a participant's assets to them).

THE "LOST AND FOUND" DATABASE

Section 303 of Secure 2.0 directs the U.S. Department of Labor (DOL) to create a national online searchable lost and found database that plan participants who have lost track of their retirement benefits can use to search for the contact information of their plan administrator. The DOL is seeking more than $4.5 million in funding in fiscal year 2024 in order to implement this legislation. While the law stipulates that the database be implemented by December 2024, some industry experts are cautious that it will take additional time for the DOL to implement. According to Norma Sharara, Managing Director in BDO's National Tax Office, "Progress is being made, and the DOL has requested the needed appropriations from Congress, but the funding has not yet been approved. And even once it is, the development process will be lengthy."

IN THE MEANTIME

While the database development is in process, there are several existing resources that plan sponsors may utilize to address their on-going fiduciary responsibility to track missing participants. For immediate and specific sponsor needs (such as if a plan sponsor is terminating a plan), the Pension Benefit Guaranty Corp (PBGC) has a voluntary missing participants **program** that is available for sponsors of certain plan types, including defined contribution [DC] plans. Plan sponsors can also follow the **DOL** and **IRS** guidelines for locating missing participants as a best practice, regardless of the impending changes.



A NEW LEVEL OF AUTOMATIC PORTABILITY

Section 120 of the Act calls for the adoption of automatic rollovers of retirement plan assets from an employee's account into a new employer's plan after termination of employment. The law currently allows for an employer to roll over this distribution into a default IRA if the account balance is at least $1,000 and the participant does not affirmatively elect otherwise. The Act's provision enhances portability by allowing the plan sponsor to now transfer the former employee's default IRA assets (established at termination) into the participant's new employer's plan. The provision both curtails asset leakage from ERISA plans and helps alleviates the missing participant issue.

In a related provision, **Section 304** of Secure 2.0 increases the dollar limit for plan sponsors to automatically cash out a former employee's retirement plan from $5,000 to $7,000 starting in 2024. While the law does not mention automatic portability in relation to this provision, the higher limit will allow a higher percentage of participant accounts to be eligible for automatic rollovers.

VENDOR ASSISTED ROLLOVERS

Plan sponsors may choose to work with a vendor for assistance in implementing automatic rollovers. One current option is the **Portability Services Network** that was created in collaboration with some of the key retirement plan industry providers and Retirement Clearinghouse (RCH).

MEETING YOUR FIDUCIARY OBLIGATIONS

With Secure 2.0 implementation, benefit plan administration continues to evolve. Plan sponsors seeking enhanced ways to fulfill their fiduciary duty will need to consider all available tools, both those existing/being improved and those under development.

Your BDO representative is there to assist you in navigating these changes and implementing best practices.

Mental Health Parity Compliance

In the U.S., it's estimated that more than one in five adults live with a mental illness — **that's about 57.8 million people as of 2021**. In response to the growing awareness of the importance of treatment for mental health and substance use disorders (MHSUD), the Centers for Medicaid & Medicare Services (CMS) enacted the Mental Health Parity and Addiction Equity Act (MHPAEA) of 2008.

The legislation expands on the Mental Health Parity Act of 1996 and requires health insurers and group health plans that offer MHSUD benefits to provide the same level of benefits for mental and/or substance use treatment and services that they do for medical or surgical care. The legislation also ensures that plans offered on the Health Insurance Marketplace under the Affordable Care Act (ACA) cover many behavioral health treatments and services while requiring some plans to cover MHSUD services as an essential health benefit.

Compliance enforcement related to MHPAEA is likely to increase as time goes on. That means it's more important now than ever before for organizations to comply with both federal and state parity law requirements.

As an example, the following legislative actions indicate immediate consideration:

- The DOL and the U.S. Centers for Medicare and Medicaid Services (CMS) have issued a brief summarizing their MHPAEA enforcement efforts in fiscal year 2022.
- The U.S. Department of the Treasury, the US Department of Labor (DOL) and the U.S. Department of Health and Human Services (HHS) published a **technical release** setting forth a potential approach that the agencies may take to determining the types of compiled data required of employers addressing any nonquantitative treatment limitations (NQTLs) in their health plans so as to not conflict with the MHPAEA standards regarding composition of provider networks. The agencies have requested comments on the technical release.
- An updating of the current 2013 **final MHAEA regulations** that would be effective as of 2025 that add additional layers of compliance from the agencies resulting in higher costs for employers.
- **A congressional report** authored by these three agencies detailing recent enforcement efforts and citing multiple employee benefit plans that have violated the MHPAEA.

BDO's Mental Health Parity Compliance team can help you address common challenges like:

- Determining whether your organization is obligated to offer MHSUD services as a plan sponsor under MHPAEA.
- Assessing whether your current or prospective benefits offerings are compliant with MHPAEA requirements.
- Acquiring a certification of compliance for MHPAEA.
- Adding procedures to your current corporate compliance policies and procedures to include mental health parity alignment.

If you're experiencing any of these challenges, our **Mental Health Parity Compliance** team may be able to help.

OUR APPROACH

Our team of experienced professionals is ready to help ensure your organization is compliant with MHPAEA requirements.

Benefits Assessment: Our team of regulatory professionals and experienced industry professionals will evaluate quantitative and non-quantitative aspects of your current or prospective employee benefits.

Testing & Comparative Analyses: Our team can help you prepare Non-Quantitative Treatment Limitations (NQTL) comparative analyses documentation, as well as perform Quantitative Treatment Limit (QTL) testing for potential Department of Labor (DOL) and CMS audits.

Process & Procedure Development: We'll guide you through updating or creating processes and procedures for your current corporate compliance plan to include mental health parity alignment.

Compliance Certification: Once aligned with requirements, we can provide a certification of benefits compliance under MHPAEA.

OUR SERVICES

- Risk & Regulatory Compliance
- Compliance Program Gap Assessment
- Employee Benefit Plan Audit
- Benefit Plan Design

CLIENT OUTCOMES

- Ensure you are in compliance with the latest MHPAEA requirements
- Generate documentation showing your compliance
- Mitigate the risk of **monetary penalties**, up to $110 per day for failure to submit documentation upon request, and $100 per day in excise taxes, as a result of DOL, CMS, and state-imposed enforcement fines

WHY CHOOSE BDO

We have the experience. Our team is made up of knowledgeable consultants and former healthcare industry leaders who've been in your shoes. We work with organizations of various sizes and types and know the importance of ensuring your company is compliant with all applicable regulations.

We manage change so you don't have to. Compliance with changing requirements can be confusing. Our experienced team is by your side to walk you through every phase of satisfying MHPAEA obligations.

We make sure you're prepared. Our team will work with you to create or add to processes and procedures for compliance to include mental health parity alignment. We'll provide you with testing documentation and compliance assertion in the event of an audit.

Ready to assess whether your benefits are MHPAEA compliant? Reach out to a BDO professional today.

Plan Sponsor Alert: Tips for Effective HSA Plan Provider Selection

As the demand for Health Savings Accounts (HSAs) continues to grow, employers are increasingly adding these tax-advantaged personal savings accounts to their benefits packages. But just as they would when selecting and setting up a 401(k) offering, employers need to consider introducing a set of standards and processes for HSA provider selection and monitoring. **Guidance** from Department of Labor's Employee Benefits Security Administration (EBSA) is a great starting point, but some HSA features require special consideration.

In this article — the second article in our **two-part series on HSAs on HSAs** — BDO highlights best practices and key considerations when choosing an HSA provider.

START WITH THE EBSA'S TIP SHEET

Generally, HSAs are not regulated by EBSA; however, many of EBSA's tips for selecting and monitoring service providers are transferrable to the HSA selection process.

Plan sponsors should start by considering the services needed to operate the HSA. They should also review whether the HSA vendor can provide bundled benefit offerings as this may provide cost savings for the organization. Utilizing one platform for the HSA and 401(k) offerings may streamline your benefits lineup and help employees understand how these accounts complement each other.

In some ways, plan sponsors should approach this like a hiring process. Understanding the terms of the contract signed with an HSA provider is critical, as is having a written record of the process used to hire the HSA provider. And just like you would for 401(k) service providers, evaluating your HSA vendor on a regular basis can help ensure your organization gets the most out of the service.

KEEP AN EYE ON KEY TRENDS

Knowing what other employers are looking for in an HSA provider can help you understand what is available and which features matter most to your organization. The Plan Sponsor Council of America (PSCA)'s fourth annual **HSA benchmarking report** is a helpful resource that includes trend statistics on must-haves for today's HSA vendors.

According to the PSCA's report, nearly 90 percent of respondents used a consultant or benefits broker to help develop their HSA program. The best consultants will provide trend information, gain an understanding of your organization's demographics and help you decide which features might work best.

The PSCA report outlines the three most important features reported by plan sponsors:

- Having a debit card (36 percent),
- 24/7 customer service (23 percent), and
- Employee engagement/communication (15 percent).

Another area covered in the PSCA report was whether to offer investment options as part of your HSA program. The PSCA report showed that 61 percent of respondents offer investment options, and large employers are twice as likely to offer them vs. smaller employers. Ultimately, the decision to provide investment options should be based on your plan's universe of participants and their specific needs.

BDO INSIGHT: Avoid Triggering ERISA Compliance

Nearly 20 years ago, the Department of Labor (DOL) issued **Field Assistance Bulletin 2004-01**, which outlines the conditions that would keep HSAs out of the realm of employee welfare benefit plans covered by Employment Retirement Income Security Act (ERISA). Plan sponsors should ensure they understand these rules to avoid any potential issues with ERISA law.

Generally, HSAs fall outside ERISA rules if employers avoid the following:

- Requiring contributions (i.e., employee contributions must be completely voluntary)
- Limiting employees' ability to move funds to another HSA
- Imposing conditions on employees' use of the funds
- Making or influencing investment decisions
- Saying that the HSA is subject to ERISA standards
- Taking payment or compensation in connection with the HSA

If you would like to learn more about selecting an HSA provider for your organization, your BDO representative is able to help.

CONTACT:

BETH LEE GARNER
Assurance Managing Principal, Employee Benefit Plan Audits and ERISA Services Plan Audits
404-979-7143 / bgarner@bdo.com

NICOLE PARNELL
Managing Director, Retirement Plan Services Leader
757-640-7291 / nparnell@bdo.com

MICHAEL BELONIO
Assurance Director, Northeast Region Practice Leader
212-404-5516 / mbelonio@bdo.com

MARY ESPINOSA
Assurance Principal, West Region Practice Leader
714-668-7365 / mespinosa@bdo.com

JODY HILLENBRAND
Assurance National Technical Principal, Southwest Region Practice Leader
210-424-7524 / jhillenbrand@bdo.com

PAM SLAGH
Audit Director, Central Region Practice Leader
616-802-3419 / pslagh@bdo.com

JOAN VINES
Managing Director, National Tax Compensation & Benefits
214-701-6122 / jvines@bdo.com

NORMA SHARARA
Managing Director, National Tax Compensation & Benefits
202-981-3973 / nsharara@bdo.com