October 27, 2021

MAYER | BROWN

Benefits & Compensation University

Latest ERISA Developments & Trends

Erin K. Cho
Partner
+1 202 263 3066
erincho@mayerbrown.com

Maureen J. Gorman
Partner
+1 650 331 2015
mgorman@mayerbrown.com

Hillary E. August
Associate
+1 312 701 8135
haugust@mayerbrown.com

Joseph A. Lifsics
Associate
+1 312 701 7233
jlifsics@mayerbrown.com

Today's Presenters

Erin K. Cho

Partner
Washington DC
+1 202 263 3066
erincho@mayerbrown.com

Erin's practice focuses on ERISA Title I matters. She has extensive experience advising financial institutions, asset managers, insurance companies and other retirement plan service providers with respect to the many and varied services and financial products (including complex structured products and derivatives) they offer to US pension plans. She counsels plan sponsors on all aspects of ERISA fiduciary compliance, including plan governance, plan expense issue and the selection and monitoring of plan investment options.

Maureen J. Gorman

Partner
Palo Alto
+1 650 331 2015
mgorman@mayerbrown.com

Maureen is a Firm Practice Leader of the Employment & Benefits practice who focuses on executive compensation and employee benefits matters. Her work includes advising on tax and benefit issues in both domestic and international contexts, counseling on ERISA fiduciary issues, controversy work involving IRS and DOL audits, and all nature of transactional work, including de-risking transactions and M&A. Her work frequently requires interdisciplinary efforts with corporate, securities and tax specialists.

Hillary E. August

Associate
Chicago
+1 312 701 8135
haugust@mayerbrown.com

Hillary advises clients on a wide range of issues involving employee benefits, including the design, implementation, communication, administration and amendment of tax-qualified retirement plans, executive compensation arrangements, and health and welfare plans and policies. She also counsels plan fiduciaries on their obligations under ERISA and advises on risk mitigation. Hillary has represented plan sponsors, fiduciaries and service providers in fiduciary breach matters involving retirement plan investments, plan fees and expenses, and employer stock.

Joseph A. Lifsics

Associate
Chicago
+1 312 701 7233
jlifsics@mayerbrown.com

Joe's practice focuses on ERISA Title I matters. He advises clients on ERISA issues relating to pension investments and private funds. He assists with the structuring and formation of funds, including the drafting of fund documents and negotiates with prospective investors regarding their ERISA-related comments to fund documents and side letters. Additionally, Joe helps fund sponsors maintain their funds as qualifying for an exception to holding plan assets under ERISA, including the structuring of the underlying investments of such funds.

Agenda

- Cybersecurity considerations for benefit plans
- ESG investing and proxy voting rules
- Lifetime income disclosure rules
- Handling missing participant issues

Cybersecurity

- Retirement accounts are attractive targets for cyber-enabled fraud
- Plans hold more than $9.3 trillion of assets
  - Plan participants generally check their retirement accounts less frequently than personal banking, credit card, or other financial accounts
  - As a result, there can be a delay before attacks on retirement accounts are discovered, and by the time an incident is identified, it may be too late
  - Plans also permit electronic access to funds and rely on outside service providers who provide additional access points for breach

Cybersecurity Litigation

- Since 2018, lawsuits have been filed alleging claims under ERISA regarding cyberattacks
- The litigation has raised important questions about the extent of fiduciary responsibility regarding:
  - Cybersecurity practices for plans and important transactions (e.g., distributions, changes to approved bank accounts)
  - The duty to monitor cybersecurity practices used by service providers

Cybersecurity Litigation

***Leventhal v. MandMarblestone Grp. LLC*, No. 18-CV-2727, 2019 WL 1953247, (E.D. Pa. May 2, 2019)**

- A plan participant alleged that the plan's TPA and investment provider failed to prevent "unknown criminal(s)" from withdrawing more than $400,000 from the participant's account
- Court sided with the participant at motion to dismiss stage, holding that TPA and the investment provider were fiduciaries and plaintiffs' fiduciary breach claims could proceed
- *Takeaway:* Decision suggests cybersecurity claims are viable at least at motion to dismiss stage

Cybersecurity Litigation

Leventhal v. MandMarblestone Grp. LLC, No. 18-CV-2727, 2019 WL 1953247, (E.D. Pa. May 2, 2019)

- Court rejected the providers' argument that there was no "breach of fiduciary duty under ERISA because there is no duty to ensure the security of Plaintiffs' IT systems," and also rejected the providers' argument that they had "no duty to prevent forgeries."
- Court agreed with the participant and the plan that the providers "failed to act with the requisite prudence and diligence where they saw the 'peculiar nature' and high frequency of the withdrawal requests that were to be distributed to a new bank account. . . ."
- Court agreed with the plaintiffs that "[d]efendants failed to implement 'the typical procedures and safeguards' used to notify Plaintiffs of the strange requests and/or verify the requests."

Cybersecurity Litigation

***Berman v. Estee Lauder Inc.*, No. 3:19-cv-06489 (N.D. Cal. filed Oct. 9, 2019)**

- Participant sued her employer, the plan's fiduciary committee, the recordkeeper, and the plan's custodian
- Plaintiff alleged that over the course of two months, "an unknown person or persons . . . withdr[ew] a total of $99,000 in three separate unauthorized distributions from her account," and that unauthorized distributions from the plaintiff's account had been made to three different bank accounts
- On March 5, 2020, it was reported that the parties had agreed to settle the litigation

Cybersecurity Litigation

***Berman v. Estee Lauder Inc.*, No. 3:19-cv-06489 (N.D. Cal. filed Oct. 9, 2019)**

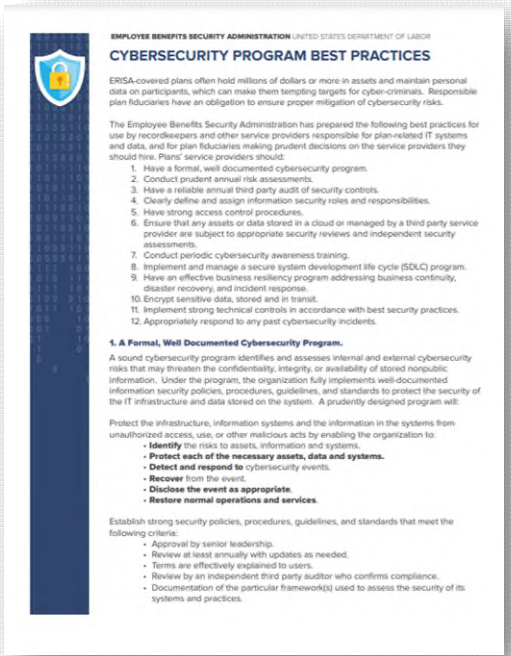
- Plaintiff alleged that defendants breached their fiduciary duties of loyalty and prudence by failing to –
  - confirm authorization for distributions with the plan participant before making distributions
  - provide timely notice of distributions to the plan participant by telephone or email
  - identify and halt suspicious distribution requests;
  - establish distribution processes to safeguard plan assets against unauthorized withdrawals
  - monitor other fiduciaries' distribution processes, protocols, and activities

Cybersecurity Litigation

Bartnett v. Abbott Laboratories, No. 1:20-cv-02127 (N.D. Ill. filed Apr. 3, 2020)

- Plaintiff alleged that defendants (Abbott Laboratories, Abbott Corporate Benefits, Marlon Sullivan, and Alight Solutions) breached their fiduciary duties of loyalty and prudence
- In October 2020 and February 2021, the court dismissed the claims against the plan sponsor and named fiduciary on the grounds that there was no evidence of fiduciary breach or a failure to monitor
- The court rejected the recordkeeper's arguments that it did not act as a fiduciary to the plan. The recordkeeper's ability to disburse the funds demonstrated that it exercised discretionary control or authority over plan assets
- The court permitted the breach of fiduciary duty claims against the recordkeeper to proceed

DOL Guidance
Service Providers



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

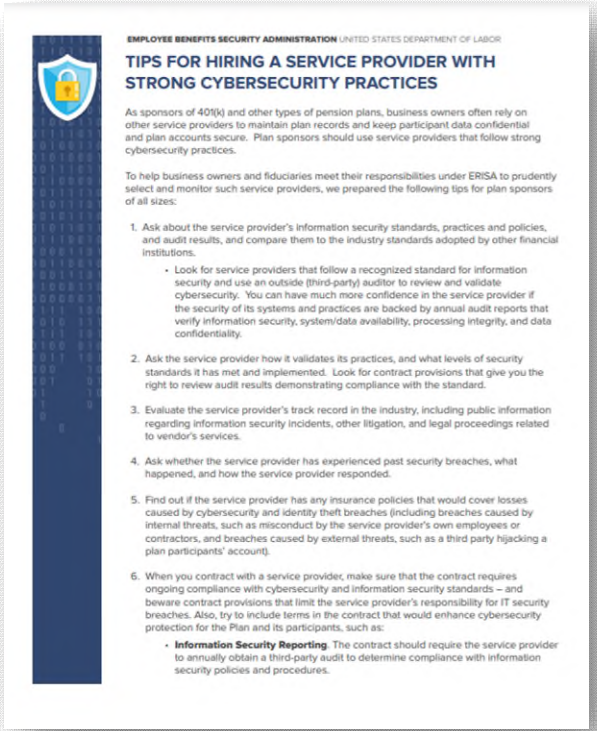
- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate.**
- **Restore normal operations and services.**

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

DOL Guidance
Plan Sponsors



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

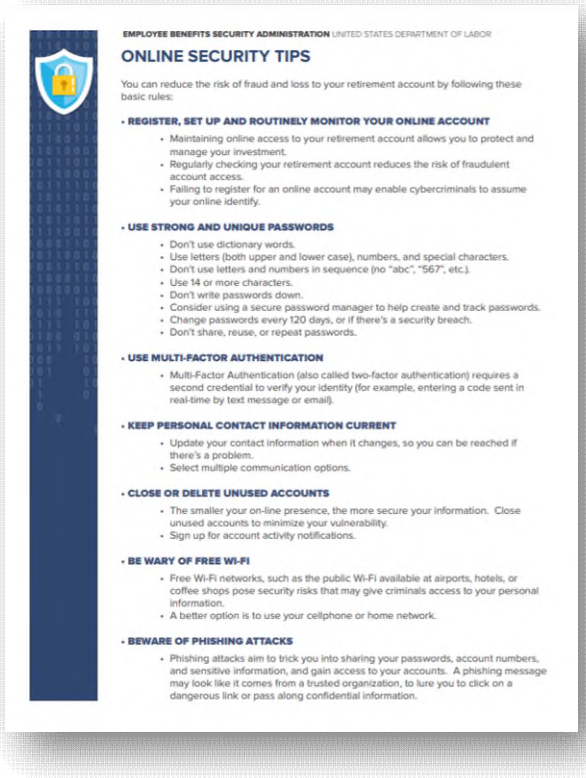
As sponsors of 401(k) and other types of pension plans, business owners often rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of all sizes:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.
   - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.
2. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.
3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).
6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants, such as:
   - **Information Security Reporting**. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

- Key Questions to Ask Service Providers
- Provisions DOL Expects in Contracts
  - Third-party audit
  - Provisions on use and sharing of information
  - Notification
  - Compliance with all privacy laws
  - Consider insurance coverage

DOL Guidance
Participants



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

ONLINE SECURITY TIPS

You can reduce the risk of fraud and loss to your retirement account by following these basic rules:

- **REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT**
  - Maintaining online access to your retirement account allows you to protect and manage your investment.
  - Regularly checking your retirement account reduces the risk of fraudulent account access.
  - Failing to register for an online account may enable cybercriminals to assume your online identify.
- **USE STRONG AND UNIQUE PASSWORDS**
  - Don't use dictionary words.
  - Use letters (both upper and lower case), numbers, and special characters.
  - Don't use letters and numbers in sequence (no "abc", "567", etc.).
  - Use 14 or more characters.
  - Don't write passwords down.
  - Consider using a secure password manager to help create and track passwords.
  - Change passwords every 120 days, or if there's a security breach.
  - Don't share, reuse, or repeat passwords.
- **USE MULTI-FACTOR AUTHENTICATION**
  - Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).
- **KEEP PERSONAL CONTACT INFORMATION CURRENT**
  - Update your contact information when it changes, so you can be reached if there's a problem.
  - Select multiple communication options.
- **CLOSE OR DELETE UNUSED ACCOUNTS**
  - The smaller your on-line presence, the more secure your information. Close unused accounts to minimize your vulnerability.
  - Sign up for account activity notifications.
- **BE WARY OF FREE WI-FI**
  - Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops pose security risks that may give criminals access to your personal information.
  - A better option is to use your cellphone or home network.
- **BEWARE OF PHISHING ATTACKS**
  - Phishing attacks aim to trick you into sharing your passwords, account numbers, and sensitive information, and gain access to your accounts. A phishing message may look like it comes from a trusted organization, to lure you to click on a dangerous link or pass along confidential information.

- Set-up your account, good password behavior, keep contact info current
- Council believes participants share responsibility
- Consider providing to participants?

Executive Order on Cybersecurity

- Issued May 12, 2021
- Allows sharing of info with federal government
- Baseline standards for software vendors
- Cybersecurity review board
- Create standard playbook and set of definitions for cyber incidents

Takeaways for Plan Sponsors

- The tips include steps that plan sponsors and administrators might take with respect to diligence of, and contracting with, plan service providers include:
  - Compare the provider's cybersecurity program to industry standards
  - Seek providers that engage a third-party auditor to annually review and validate its cybersecurity program
  - Ask about past security breaches and how they responded
  - Ask about the provider's insurance policies

Takeaways for Plan Sponsors

  - Include in the contract how much time the provider has to provide notice of a security breach and require the provider investigate and reasonably address the cause of the breach
  - Carefully review limitations of liability causes

- In taking this prescriptive approach, these guidelines may serve as a standard to determining whether a plan fiduciary acted in a prudent manner
- The guidance appears intended to apply to retirement plans as it regularly refers to the security of retirement plans and retirement plan assets. However, in key places, the guidance refers more generally to "ERISA-covered plans" and as a result, even if unintended, it can be broadly read to also apply to health and welfare plans

Takeaways for Plan Sponsors

- Plan fiduciaries should immediately review their current hiring practices and service provider contracts and evaluate whether they meet the suggested standards
  - Provisions that limit the service provider's liability and obligations in the event of a breach as well as participant guarantee and notice provisions should be carefully scrutinized
- The tips are aimed to assist fiduciaries with their monitoring duties
  - Regular (annual) review of third-party audits, periodic review of other information on the provider's track record and regular RFPs to ensure the sophistication of security methods relative to competitors and industry standards

Takeaways for Plan Sponsors

- Until the DOL issues further clarification, fiduciaries for health and welfare plans may need to consider reconciling the tips with other security guidance that already applies to such plans, for example, HIPAA's privacy and security standards and various data security breach laws
- Plan sponsors should also be educating plan participants about the guidance and emphasize the importance of strong password use, phishing awareness, updating personal contact information and monitoring accounts

Background: ESG and Proxy Voting Rule

- On October 14, 2021, the DOL proposed a new regulation relating to ESG investing and proxy voting
  - The DOL issued slightly different guidance on these topics under each of the Clinton, Bush, Obama and Trump administrations
    - The basic principal that economics cannot be sacrificed for policy preferences has remained constant
    - Shifts in tone, points of emphasis, and differences on the margins
  - Until 2020, the guidance has been sub-regulatory (field assistance and interpretive bulletins)

Background: ESG and Proxy Voting Rule

- In 2020, the DOL issued regulations on both ESG and proxy voting shortly before President Trump left office
  - The DOL expressed skepticism regarding the importance of ESG factors and placed an emphasis on scenarios where plan shareholder rights should **not** be exercised
- President Biden issued two executive orders directing the DOL to review these regulations
- The DOL issued a non-enforcement policy of the Trump-era regulations in March of 2021

2020 ESG Regulations (Trump)

- Originally singled-out ESG investing as facing additional scrutiny
- Final rule focused on "pecuniary" vs. "non-pecuniary factors"
- Fiduciaries required to base their investment decisions solely on pecuniary factors
  - Non-pecuniary factors are allowed only as a tie-breaker
    - If the plan fiduciary is unable to distinguish between investments based on pecuniary factors
    - Documentation requirement
- Prohibition on selecting a QDIA if the investment option's objectives, goals or principal investment strategies consider non-pecuniary factors

Proposed Regulation: ESG

- More welcoming of ESG, but financial factors are still key
- Fiduciaries cannot choose investments based on policy preferences if it does not make economic sense.
- However, the proposal states that climate change and other ESG factors may often be material economic considerations and provided examples:
  - Climate-change (both direct effects and associated government regulations)
  - Governance factors (e.g., board composition, accountability and transparency)
  - Workforce practices (e.g., diversity, retention and training practices)

Proposed Regulation: ESG

- Collateral ESG factors can be used as a tie-breaker
  - DOL requested comment on whether to restrict the kinds of collateral factors that can be used (e.g., those that are within the shared interests of the participants)
- More permissive standard for when a "tie" occurs
  - The investments "equally serve the financial interests of the plan over the appropriate time horizon"
  - Investments can be economically distinguishable, but equally appropriate for the plan's investment portfolio
- No documentation requirement

Proposed Regulation: ESG

- Collateral factors can be used as a tie-breaker when selecting designated investment options in a participant-directed plan (e.g., a 401(k) plan)
  - The nature of such collateral factors must be "prominently displayed"
  - 404a-5 disclosure is the natural place to provide this disclosure
- A fund can be chosen as a QDIA despite its consideration of collateral ESG factors
  - Must be financially prudent and otherwise meets the QDIA regulations

Proposed Regulation: Proxy Voting

- Fiduciary duties extend to the management of the plan's proxies and other shareholder rights
- Proxies should generally be voted upon unless doing so would not be in the plan's best interest (e.g., due to the prohibitive cost involved)
- Removes language from the 2020 rule that fiduciaries need not vote every proxy
  - DOL explained that while this is technically true, it worried that this would be misconstrued as a directive not to vote
- Specific documentation requirement is eliminated

Proposed Regulation: Proxy Voting

- When considering whether and how to vote a proxy/exercise shareholder rights, a fiduciary must:
  - Act solely in accordance with the economic interests of participants and beneficiaries
  - May not subordinate their financial interests to any other objective
  - Consider relevant costs involved
  - Evaluate material facts that form the basis for the proxy vote or exercise of shareholder rights
  - Exercise prudence and diligence in selecting and monitoring of service providers that exercise or otherwise assist with the exercise of shareholder rights

Proposed Regulation: Proxy Voting

- Fiduciaries may develop guidelines to assist in deciding which proxies to vote upon
  - Must be prudently designed to provide benefits to plan participants and beneficiaries and defray reasonable administrative expenses
  - Must periodically review such policies
    - (prior guidance indicated ~2 years)
  - Unlike the 2020 Trump Proxy rule, there are no safe harbor sample policies
  - Fiduciaries can always decide to vote (or not vote) a given proxy regardless of what the policy says if it believes that doing so would be in the best interests of the plan

Proposed Regulation: Proxy Voting

- For a pooled investment vehicles subject to ERISA with multiple ERISA investors, the manager must attempt to reconcile conflicting voting policies
  - For proxies, the manager must vote in proportion to each ERISA investors' respective interest in the vehicle
  - Alternatively, the manager can require plans to review and approve of the manager's policy prior to investing

ESG and Proxy Takeaways

- DOL has clearly shifted towards viewing ESG investing in a favorable light
- **Economics remain key**
  - Collateral ESG factors or policy preferences cannot outweigh economic considerations
- Plan fiduciaries should prepare to begin incorporating an analysis of economic ESG factors as part of their investment process
- Fiduciaries should generally vote proxies unless it is not in the plan's best interest
- Comments on the proposed rule are due December 13, 2021

Missing Participant Issues
Background

- DOL issued 3 pieces of guidance in January 2021:
  - Missing Participants – Best Practices for Pension Plans
  - Compliance Assistance Release No. 2021-01, Terminated Vested Participants Project Defined Benefit Pension Plans
  - Field Assistance Bulletin No. 2021-01, Temporary Enforcement Policy Regarding the Participation of Terminating Defined Contribution Plans in the PBGC Missing Participants Program
- Missing/nonresponsive participant is a participant, beneficiary, or alternate payee who is: (1) entitled to a benefit but cannot be located; or (2) sent a lump-sum check that goes uncashed and becomes stale-dated

Missing Participant Issues
Background

- Pension Benefit Guaranty Corporation (PBGC) Missing Participants Program
  - Accepts transfers of benefits for missing participants in terminating defined benefit and – since 2017 – defined contribution plans
  - PBGC conducts search for missing participants/beneficiaries
- Prior DOL guidance:
  - FAB 2004-02: Fiduciary Duties and Missing Participants in Terminated Defined Contribution Plans
  - Safe Harbor Regulations for Terminated Individual Account Plans (2006)
  - FAB 2014-01: Fiduciary Duties and Missing Participants in Terminated Defined Contribution Plans

Missing Participant Issues
Background

- Increasing focus by DOL investigators on whether employers and plan service providers established necessary procedures to search for and locate missing participants
- This became the DOL's Terminated Vested Participant Project (TVPP)
- Ultimately, the DOL issued its three new pieces of guidance on January 12, 2021

Missing Participant Issues
2021 Best Practices Guidance

- Lays out potential "red flags" and guidance at a variety of stages:
  - Ward off problems by maintaining accurate census information
  - Implement effective communication strategies
  - Take a variety of steps to search for missing participants
  - Document procedures and actions
- Fiduciaries are not required to engage in every best practice
  - Consider what practices will yield the best results
  - Consider the size of a participant's accrued benefit and account balance in light of search costs

Missing Participant Issues
2021 Best Practices Guidance

- Red flags:
  - More than a "small number" of missing or nonresponsive participants or TVPs at retirement age who haven't started receiving benefits
  - Missing, inaccurate, or incomplete contact information, census data, or both
  - Absence of sound policies and procedures for handling returned mail
  - Absence of sound policies and procedures for handling uncashed checks
- *Key Takeaways*:
  - Audit census information regularly
  - Work with plan recordkeeper/review recordkeeper agreement and processes

Missing Participant Issues
2021 Best Practices Guidance

- Maintaining accurate census information:
  - Contact participants and beneficiaries to confirm or update contact information
  - Make it easy for participants to update their contact information
  - Flag undeliverable mail, email, and uncashed checks for follow-up
  - Review and update records around major corporate events
- *Key Takeaways*:
  - Contact change requests/reminder to update information in communications
  - Request social media contact information

Missing Participant Issues
2021 Best Practices Guidance

- Communicating effectively with participants:
  - Use plain language and offer non-English assistance
  - Encourage contact through website and toll-free numbers
  - Make plan correspondence easily recognizable
  - Inform participants about consolidating defined contribution/IRA accounts
  - Build in steps during on-boarding/exit process to confirm information
- *Key Takeaways*:
  - Confirm recordkeeper/service provider capabilities
  - Discuss how mailings will be labeled

Missing Participant Issues
2021 Best Practices Guidance

- Searching for missing participants:
  - Draw on related plan and employer/payroll information
  - Check with designated beneficiaries/emergency contacts
  - Use free or proprietary online search tools, commercial locator services
  - Review public records databases, obituaries
  - Register the participant on public and private pension registries
- *Key Takeaways*:
  - Determine which steps to take in light of plan size, balance at issue, fiduciary duties
  - Consider privacy implications

Missing Participant Issues
2021 Best Practices Guidance

- Documenting policies and procedures:
  - Reduce the plan's policies and procedures to writing
  - Document key decisions and the steps/actions taken to implement policies
  - Ensure recordkeeper is performing agreed upon services
  - Work with the recordkeeper to identify shortcomings in the recordkeeping process
- *Key Takeaways*:
  - Potential policies: guidance for handling undeliverable/returned mail, conducting regular census audit, collecting census information at hire/termination
  - Policies, procedures, and records may help in the case of a DOL audit

Missing Participant Issues
CAR 2021-01

- Internal DOL memo describing the approach DOL regional offices should take under the Terminated Vested Participants Project
- Outlines investigative approach:
  - Why investigations are opened
  - Information sought during investigation
  - Errors the DOL looks for in an investigation
  - How the DOL closes an investigation

Missing Participant Issues
FAB 2021-01

- DOL will not pursue fiduciary breach claims against fiduciaries or Qualified Termination Administrators of abandoned plans for transferring missing participant accounts to PBGC Missing Participants Program for terminating defined contribution plans
- Temporary guidance and only an enforcement policy
- Can be used if fiduciaries:
  - Follow FAB 2021-01
  - Act with a good faith, reasonable interpretation of ERISA Section 404
  - Meet other requirements

Lifetime Income Disclosure

- ***Headline:*** On July 26, 2021, the DOL issued FAQs that clarify the deadlines for the provision of the new lifetime income disclosure illustrations required by the SECURE Act
- ***Background:*** ERISA Section 105(a), as revised by the PPA, requires plan administrators of individual account plans to provide benefit statements at least annually; provided that in the case of a plan with participant-directed investments, benefit statements must be provided at least quarterly
- In 2013, the DOL issued an Advance Notice of Proposed Rulemaking (ANPR) in which it indicated that it was considering issuing a proposed rule mandating lifetime income illustrations on benefit statements and suggested a possible framework for calculation thereof

The SECURE Act

- **The Secure Act** enacted in 2019 created a new requirement that plan administrators of individual account plans include in benefit statements a lifetime income disclosure:
  - Under the Act, such disclosure must be provided at least annually and set forth the monthly amount of a QJSA and of a single life annuity that are each actuarially equivalent to the participant's total account balance
  - The life time streams are to be calculated based on assumptions to be issued by the DOL
- **The SECURE Act** tasked the DOL with issuing within 1 year of enactment of the SECURE Act:
  - An interim final rule
  - Assumptions for converting account balances to lifetime income streams
  - A model disclosure

  The Act provides that the new disclosure requirement applies to benefit statements issued more than 12 months after the last of those three pieces of DOL guidance is issued

The Interim Final Rule

The Interim Final Rule. On September 18, 2020, the DOL issued an Interim Final Rule that sets forth the elements for meeting the new lifetime income disclosure requirement created by the SECURE Act

- According to the DOL, the new Interim Final Rule,
  - satisfies each of the three requirements imposed on the DOL by the Act,
  - is effective on September 18, 2021
  - applies to pension benefit statements furnished after such date

The Interim Final Rule
Actuarial Assumptions

- The SECURE Act requires the DOL to prescribe the actuarial assumptions to be used for purposes of projecting the lifetime income streams (a QJSA and a single life annuity) that must be provided
- The IFR stipulates that calculations be based on the following assumptions:
  - That payment commences on the last day of the period covered by the statement
  - That as of that date the participant is age 67 (or the participant's actual age if older on that date)
  - In the case of the QJSA illustration, that the participant is married and that the spouse is the same age as the participant and that the survivor percentage is 100%
  - An interest rate equal to the 10-year constant maturity Treasury (CMT) securities yield rate for the first business day of the last month of the period to which the benefit statement relates
  - The applicable mortality table under Code section 417(e)(3)(B)
  - That the participant is 100% vested and that the account balance includes any outstanding loan other than one in default
  - No insurance load
  - No inflation adjustment

Pension Benefit Statements
Lifetime Income Illustrations

Account balance as of [DATE]	Monthly payment at 67 (single life annuity)	Monthly payment at 67 (qualified joint and 100% survivor annuity)
$125,000	$645/month for life of participant	$533/month for life of participant $533/month for life of participant's surviving spouse

- Statement must show amount of account balance as of last day of statement period

Accompanying Explanations

- The pension benefit statements must include brief understandable explanations of the assumptions underlying the illustrations; the primary purpose of the explanation is to clarify to participants that projected monthly payments are not guarantees
- The IFR includes model language that may be used to satisfy the explanation requirement
- While the explanations are required, use of the model language is optional [but see slide on limitation of liability following]
- Some flexibility in format permitted

Lifetime Income Disclosure
Limitation of Liability

- ***Limitation of Liability:*** Section 105(a)(2)(D)(iv) of ERISA provides a limitation on liability. In relevant part it states that "[n]o plan fiduciary, plan sponsor, or other person shall have any liability under this title solely by reason of the provision of lifetime income stream equivalents which are derived in accordance with the assumptions and rules [prescribed by the Secretary] and which include the explanations contained in the model lifetime income disclosure [prescribed by the Secretary]"
- Thus compliance with the DOL IFR is critical: plan fiduciaries who wish to benefit from the liability relief of ERISA section 105(a)(2)(D)(iv) must calculate the life time income illustrations in accordance with the IFR and use the DOL's model language or language that is substantially similar in all respects

Lifetime Income Disclosure
Special Rules

- **Annuities issued by insurance companies**: some defined contribution plans provide for "distribution annuities" which provide participants with periodic payments over their lives rather than lump sums. Plan administrators of plans that offer annuities through a contract with a licensed insurance company may base the two mandatory lifetime income illustrations on the terms of the insurance contract instead of the otherwise mandatory assumptions set forth in the IFR (but must still show SLA and QJSA commencing on last day of statement period and assume that participant is age 67 on that date).

- **Deferred Income Annuities**: Some plans offer participants the ability to purchase deferred income annuities (DIAs) during the accumulation phase (i.e., during the period that contributions are being made to the plan). Payment under the annuity is deferred until retirement age or even later, such as age 85. The IFR contains special disclosure rules for DIAs. *There is no model for this disclosure and, according to the DOL, the relief from liability rule does not apply.*

The New FAQs

- As noted above, the SECURE Act lifetime income disclosure requirement applies to pension benefit statements furnished more than 12 months after the latest of the issuance by the DOL of interim final rules, the model disclosure, or the assumptions prescribed by DOL
- The IFR (published on September 18, 2020) recites that it satisfies those three requirements, becomes effective on September 18, 2021, and *applies to pension benefit statements furnished after such date*
- This, however, left commentators with numerous questions regarding the specifics of the effective dates. *For example if plan provides quarterly statements, in which quarterly statement must the lifetime income disclosure first be included?*

The New FAQs

The new FAQs provide clarification:

- Participant-directed plans, which are required to deliver quarterly benefit statements, must first comply with the IFR on a benefit statement for a quarter ending within 12 months after the effective date of September 18, 2021
  - In other words, plans that must issue quarterly statements under ERISA can incorporate their initial lifetime income illustrations on any quarterly statement up to the second calendar quarter of 2022 (ending June 30, 2022)
  - Based on FAB 2007-03, it appears that the plan would have another 45 days after June 30, 2022 to deliver the statement
  - The FAQs note that whether a plan delays its first lifetime income illustration to the fullest extent permitted will depend on what makes the most sense for the plan based on its particular circumstances and current distribution cycle for benefit statements

The New FAQs

- For individual account plans that are not participant-directed (and thus are only required to provide benefit statements annually), the lifetime income illustrations must be provided on the benefit statement for the first plan year ending on or after September 19, 2021
  - For calendar year plans this would be the benefit statement for 2021
  - Per guidance issued in FAB 2007-03, the deadline for delivery will be the last date for timely filing the annual return for the applicable plan year (October 15, 2022 in the case of calendar year plans)

The New FAQs
Lingering Questions

- As noted above, back in 2013, before the SECURE Act was passed, the DOL issued an ANPR announcing consideration of a rule requiring the inclusion of lifetime income information in benefit statements issued by individual account plans. The ANPR considered requiring, *inter alia*, that plan administrators provide projected lifetime income streams (single life and QJSA if married) based on the participant's account balance *projected* to age 65
- The ANPR framework differs from the calculations required by the new IFR in a number of respects and commentators have noted that some employers and TPAs were providing lifetime income information along the lines of the ANPR (e.g., basing illustrations on projected accounts to age 65) and have asked if that approach would fulfill the requirements of the new IFR
- DOL's response is that the SECURE Act requires the provision of lifetime income illustrations that differ from the ANPR, but that the IFR specifically allows for the provision of additional life time illustrations. This seems to mean that the illustrations cited by the commentators may be included in a benefit statement along with those required by the IFR, but standing alone they will not be sufficient

The New FAQs
Lingering Questions

- The current guidance is only an interim final rule, and there has been concern that, if the DOL issues a final rule that imposes requirements, in addition to, or that are inconsistent with, those in the IFR, employers and third-party administrators will not have sufficient time to comply
- The FAQs provide that the DOL intends to issue a final rule as soon as practicable based on feedback received in the IFR, and adds, "[w]e appreciate the commenters' concerns about the burdens and challenges that could arise if the Department issues a final rule that differs materially from the IFR without sufficient transition time for plan administrators to accommodate any changes from the IFR"

Americas | Asia | Europe | Middle East

mayerbrown.com