JUNE 2021

The Retirement Times

PARTNERS
WEALTH MANAGEMENT

If You are Going to Exclude Active Funds from Your Retirement Plan Investment Lineup, Have Darn Good Reasons

The tidal surge of funds flowing from actively managed funds into passive funds reached a tipping point in 2019, when Morningstar preliminary data indicated that passive U.S. equity assets would surpass active equity assets for the first time. This inflection point was widely anticipated. Over the prior decade, active domestic equity funds leaked $1.3 trillion in outflows, while their passively managed counterparts logged nearly $1.4 trillion in the opposite direction.

Good Reasons to Include Actively Managed Funds

Actively managed funds may have higher fees than their passive counterparts, but sometimes the active management results in outperformance. This allows for higher potential returns, which can be a goal of some plan participants with higher risk tolerance, who aim to beat the market versus "own" it. Since a passive index fund is built to match the market, it will never outperform it, being virtually guaranteed to capture a little more than 100% (due to fund expenses) of market losses in every downturn.

Many active fund managers do a good job defending against — or recovering from — downturns, even if they do not outperform during bull markets. They might accomplish this with a slightly more conservative blend of investments or an ability to strategically add undervalued assets during down markets that they believe will juice returns when economic conditions improve.

A Poor Reason to Exclude Actively Managed Funds

The lower fees typically charged by passive funds are self-evidently beneficial for participants, allowing more of their contributions to grow over time. But some sponsors may be (mis)guided by self-interest when making such decisions and choose to exclude managed funds, wrongly believing that doing so will provide them ironclad protection from a 401(k)-related lawsuit.

For instance, in 2019 a $3.2 billion suit against healthcare network Community Health Systems Inc. alleged an index fund included in the organization's plan lagged its benchmark by an average of more than 9 basis points, while similar index funds lagged by approximately 1 to 2 basis points over the same period of time. And this breach of fiduciary duty, the plaintiffs claimed, led to losses in participants' retirement savings. A settlement was reached in the case. The mere provision of an index fund did not protect these fiduciaries.

Beware the Wolf in Sheep's Clothing

Plan sponsors may want to give greater scrutiny to certain actively managed funds with a low active share percentage. In some cases, such a fund could act as a closet indexer, making it more difficult for its performance to justify higher fees. And if so, may constitute a worthwhile candidate for exclusion from your plan.

No One-Size-Fits-All Answer

Constructing a retirement plan investment menu offering a wide array of choice, performance and risk characteristics requires care and consideration. But remember that there's no ERISA mandate to always select the lowest cost funds. Instead, fiduciaries should make a reasoned evaluation of whether a fund's offerings and fees are justified by its performance and value for participants.

Sources
https://www.plansponsor.com/in-depth/choosing-passive-active-funds-consider-end-result/
https://www.plansponsor.com/report-lays-out-causes-and-consequences-of-erisa-lawsuits/
https://www.morningstar.com/content/dam/marketing/shared/pdfs/Research/Fund_Flows_August2019_Final.pdf
https://www.investmentnews.com/401k-lawsuits-get-more-complex-2-170301
https://www.dol.gov/general/topic/retirement/fiduciaryresp

What is the status on allowing 401(k) match for student loan payments?

A newly proposed Senate bill by Senate Finance Chairman Ron Wyden, would enable participants to continue saving for retirement while repaying their student debt even in the event that they can't afford to make their own contributions to a 401(k) plan. This feature could be offered at the option of the employer and would apply only for expenses pertaining to higher education.

Also, student loan payments would be eligible to earn "matching" 401(k) retirement contributions from employers under a bill introduced on Thursday, April 29 by Senate Finance Chairman Ron Wyden.

You may recall that last year, the U.S. froze payments and interest for all federal student loans in response to the coronavirus pandemic. Those protections are expected to remain in place at least through the end of September.

Caveat *Guarantor*

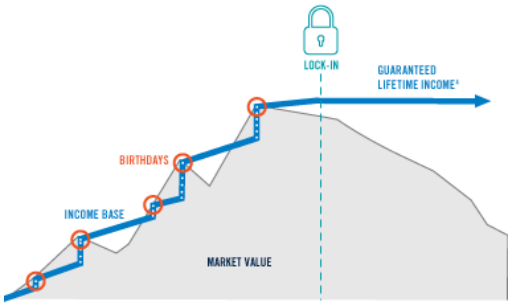
Retirement income products, or in-plan annuity options, have been available for over a decade but their utilization has been stagnant due to concerns about price, portability, and convertibility. With the recent market volatility in 2020 and recent passing of the SECURE Act, we have seen an industry push towards the research, development, and implementation of what are now referred to as "guaranteed income products."

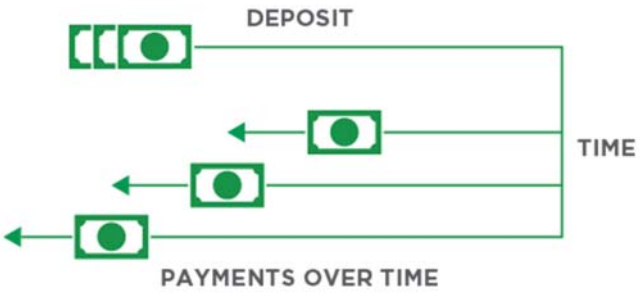
How should plan fiduciaries select and monitor these products?

Guaranteed income products bridge the gap between defined benefit and defined contribution plans. The last point of interest for these types of products occurred circa 2012, when the Department of Labor (DOL) last released guidance and brought this need to the surface. While there was little uptake at the time due to high prices and participant risk in the case of plan conversion, we are now able to revisit these concerns with some alleviation from the SECURE Act. At present fiduciaries are waiting with bated breath for the safe harbor guidance to be issued by the Department of Labor.

How do Retirement Income products work?

Many large recordkeepers and insurance companies offer, or are beginning to offer, retirement income products in one of three major categories: guaranteed lifetime withdrawal benefit (GLWB), immediate income annuities, and managed payout products.





Guaranteed Lifetime Withdrawal Benefit (GLWB)

GLWB products, true to their name, guarantee a participant to receive fixed payments for the span of their lifetime. In common practice, these products are linked to a target date series and overlayed with insurance contracts that guarantee the payout, regardless of market conditions. Participants who opt into a GLWB will make per-pay-period contributions to the product and will see it grow in coordination with the associated target date fund. The participant contributions and growth are aggregated and referred to as an income base, in which the value of the insurance contracts is then compared. At the time the participant enters retirement, the current income base is used to set fixed distributions for life.

Immediate Income Annuities

An immediate income annuity is a qualified plan distribution that allows a participant to convert their vested assets into a termed payout. This structure does not have any linkage to underlying investments but give participants the option to roll their assets directly from their target date series, or other investments, into the product to realize the fixed distribution benefit.

Managed Payout

Managed payout products, like the other two products, offer ongoing distributions to invested participants, but these payments can vary. There are two types of managed payout products. In the first type, the total assets contributed to the product will be invested and, for the agreed term, a portion of the principal and growth will be paid out as the distribution. The second type of managed payout product offers fixed payment amounts but will pay distributions up until the remaining assets are zero.

Participant Corner

ONLINE SECURITY TIPS FROM THE DEPARTMENT OF LABOR

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.
  - Common warning signs of phishing attacks include:
    - A text message or email that you didn’t expect or that comes from a person or service you don’t know or use.
    - Spelling errors or poor grammar.
    - Mismatched links (a seemingly legitimate link sends you to an unexpected address). Often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination.
    - Shortened or odd links or addresses.
    - An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information, or answers to security questions).
    - Offers or messages that seem too good to be true, express great urgency, or are aggressive and scary.
    - Strange or mismatched sender addresses.
    - Anything else that makes you feel uneasy.

- **USE ANTIVIRUS SOFTWARE AND KEEP APPS AND SOFTWARE CURRENT**
  - Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

- **KNOW HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS**
  - The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:
    - https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
    - https://www.cisa.gov/reporting-cyber-incidents

For more information on online security tips, please contact your financial professional at info@partnerswealth.com or call (630) 778-8088.

Source: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf

A Proud Member of RPAG

PARTNERS
WEALTH MANAGEMENT

Online Security Tips from The Department of Labor

- **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.
  - Common warning signs of phishing attacks include:
    - A text message or email that you didn't expect or that comes from a person or service you don't know or use.
    - Spelling errors or poor grammar.
    - Mismatched links (a seemingly legitimate link sends you to an unexpected address). Often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination.
    - Shortened or odd links or addresses.
    - An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information, or answers to security questions).
    - Offers or messages that seem too good to be true, express great urgency, or are aggressive and scary.
    - Strange or mismatched sender addresses.
    - Anything else that makes you feel uneasy.

- **USE ANTIVIRUS SOFTWARE AND KEEP APPS AND SOFTWARE CURRENT**
  - Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

- **KNOW HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS**
  - The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:
    - https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
    - https://www.cisa.gov/reporting-cyber-incidents

For more information on online security tips, , please contact your financial professional at info@partnerswealth.com or call (630) 778-8088.

Source: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf