NWCM FIDUCIARY FOCUS

EDITION 3 - 2022

RETIREMENT FIDUCIARY AND REGULATORY COMPLIANCE

REPORT BY NWCM PLAN DEPARTMENT

JUNE 2022

A summary of key fiduciary takeaways for Plan Sponsors

FOR PLAN SPONSORS

A view of Cannon Beach from Ecola State Park in Oregon.

TABLE OF CONTENTS

A NOTE FROM THE NWCM TEAM

As you may recall, the Department of Labor (DOL) issued guidance for plan fiduciaries concerning their responsibilities with respect to cybersecurity in the Spring of 2021. We previously discussed this in our **Fall 2021 edition of Fiduciary Focus**. The release hit on three major areas:

- **Online Security Tips**
- **Tips for Hiring a Service Provider with Strong Cybersecurity Practices**
- **Cybersecurity Program Best Practices**

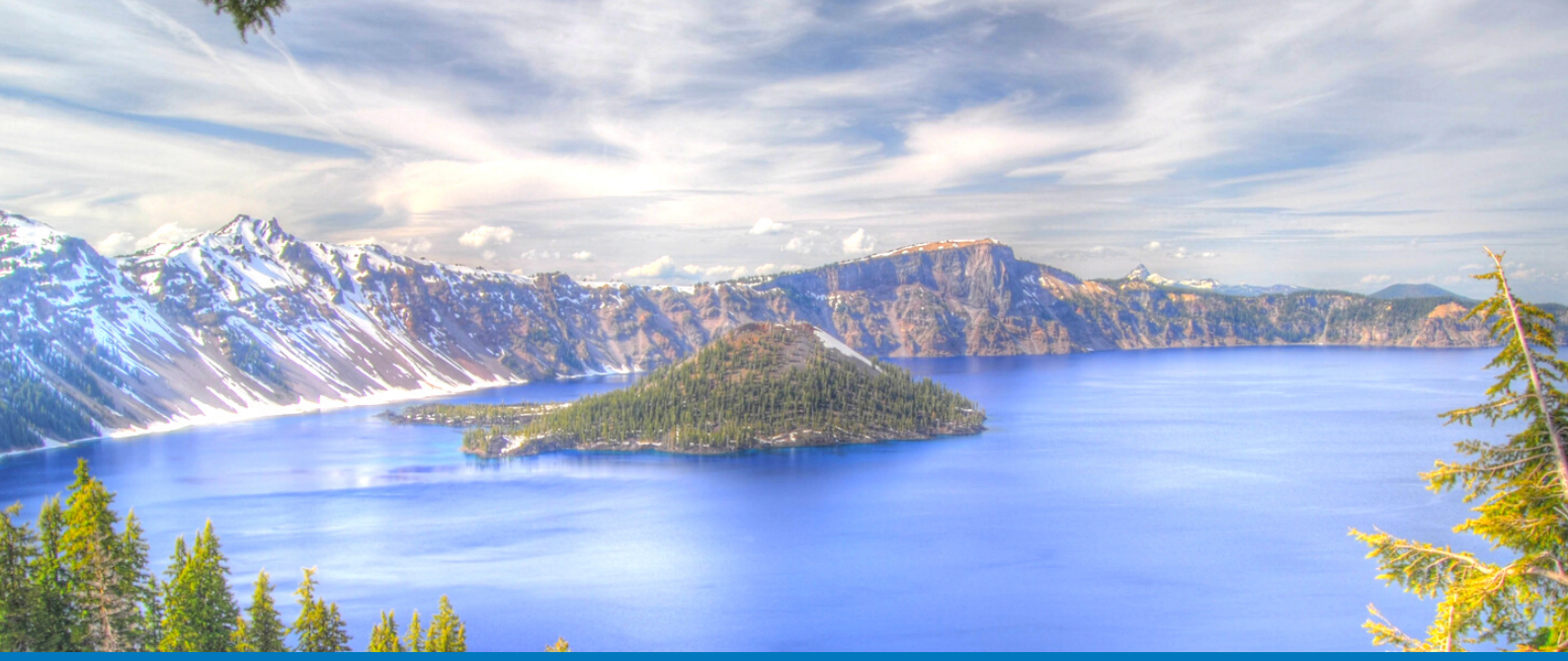
In this edition of Fiduciary Focus, we summarize each of these releases and provide plan sponsors a series of steps they can take to both improve their cybersecurity awareness and demonstrate their efforts to conform to the suggested best practices. We offer the following recommendations:

- Get educated by familiarizing yourself with the DOL releases.
- Gather relevant data that needs to be protected.
- Conduct and document an objective assessment of both your own practices and those of your retirement service plan vendors.
- Commit to making this an ongoing process.

We will also be sharing a detailed cybersecurity module with our clients to assist them in aligning their cybersecurity programs with best practices and standards.

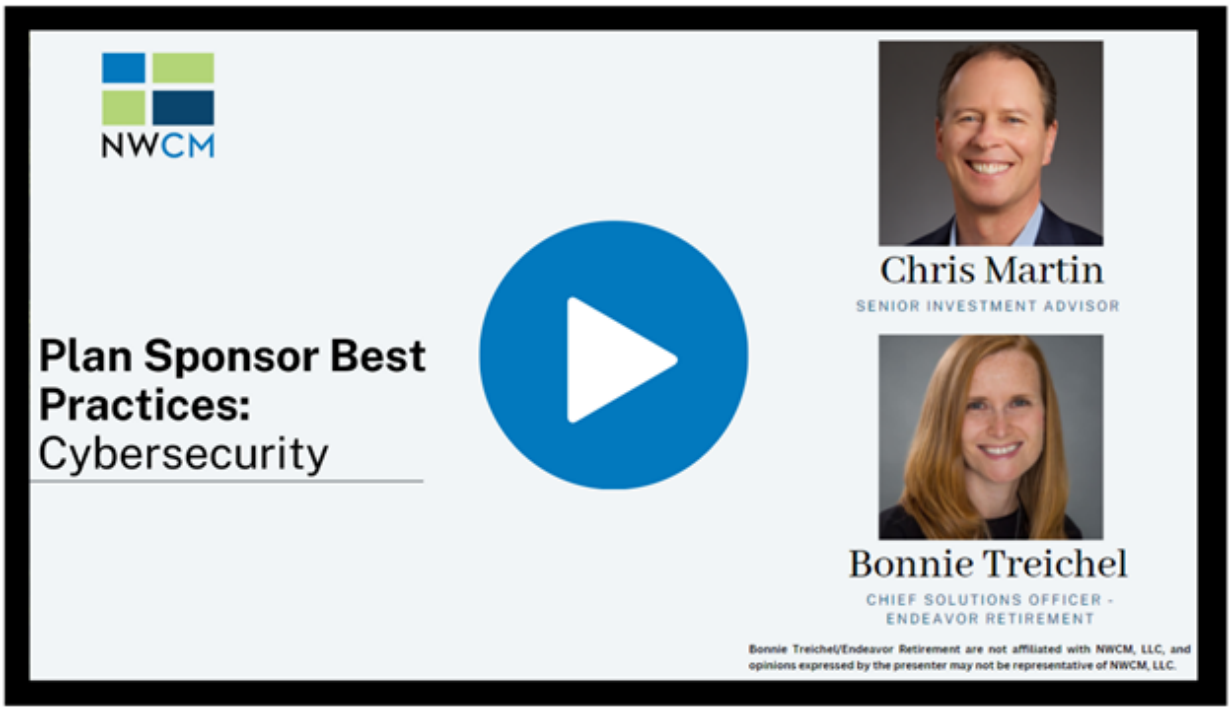
As part of our continuing effort to address developing themes affecting plan stewardship, this edition also contains a review of developments concerning cryptocurrency. We offer a summary and a **link** to our recent publication on whether cryptocurrency options belong in retirement programs. This covers the DOL's concerns about this emerging area and how plan sponsors should address them.

We appreciate your interest and invite you to reach out to your NWCM plan advisor to obtain our latest support materials on these important plan stewardship issues.



FIDUCIARY TIP: CYBERSECURITY VIDEO

In this short video, NWCM's Chris Martin speaks with Bonnie Treichel, the Chief Solutions Officer of Endeavor Retirement, about the recent DOL cybersecurity guidance. Chris and Bonnie breakdown the guidance and provide practical and actionable tips that will help plan sponsors assemble a manageable cybersecurity program.



Click **here** to watch the video and visit the NWCM Library for additional plan sponsor cybersecurity videos and resources.

Bonnie Treichel and Endeavor Retirement are not affiliated with NWCM and opinions expressed by the presenter may not be representative of NWCM.

Plan Sponsor Guide to Cybersecurity: 4 Cybersecurity Tips

In the Spring of 2021, the DOL released guidance for plan fiduciaries, recordkeepers, and plan participants on cybersecurity best practices. The goal of this guidance is to provide clarity and tips on maintaining and protecting online retirement accounts.

The guidance was provided in three forms:

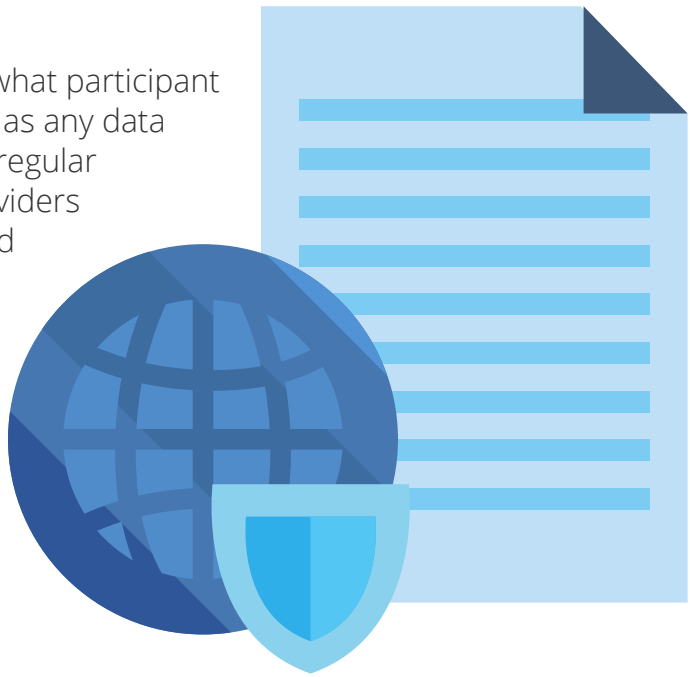
1. **Online Security Tips** – This release provided plan participants and beneficiaries guidance on how to protect their online retirement accounts and should be delivered by plan sponsors to their participants annually.
2. **Tips for Hiring a Service Provider with Strong Cybersecurity Practices** – This release provided guidance to plan sponsors on conducting service provider RFPs and how to review a service contract for cybersecurity elements.
3. **Cybersecurity Program Best Practices** – This release provided plan sponsors and recordkeepers guidance on protecting participant online retirement accounts and managing cybersecurity risk. It offers a 12-part checklist which includes best practices for recordkeepers, TPAs, and Payroll Providers.[1]

It is important to remember that the DOL's guidance applies to ALL employer-sponsored retirement plans, regardless of plan size. Although much of the guidance focuses on the selection and monitoring of service providers, the guidance also applies to the data handling and transfers done by the plan sponsor.

Below are four steps you can take to help ensure you are performing proper due diligence in protecting your plan from cybersecurity threats:

1. **Get Educated and Locate Resources to Help.** Reading the DOL's guidance and watching the videos provided by NWCM is a good first step. NWCM hosted several recent webinars covering this topic. It is also wise to coordinate with your service providers on providing cybersecurity training to your plan's participants.

2. **Gather Relevant Data.** You should identify what participant data is being held on third-party systems as well as any data which is transferred to third-party vendors on a regular basis. You should also identify which service providers receive this data. This will give an idea of how and where a data breach may occur.



(continued on the next page)

3. Conduct and Document an Objective Assessment. Conducting an honest assessment is another important step you should take. This includes identifying the service providers that handle sensitive plan data. The next step is to request from those providers a due diligence package which describes how they are meeting the 12 Best Practice steps and the specific sections in their contracts that deal with cybersecurity and related guarantees.

4. This is an Ongoing Process. You should consistently review and document the steps you are taking in preventing cybersecurity breaches on an annual basis. You should also require your service providers to advise you of any material changes they make to their cybersecurity processes once per year.

The NWCM cybersecurity module provides further training and actionable steps to guide you through this important fiduciary duty, as well as a template to document the steps you are taking. If you would like to know more, please **contact** an NWCM advisor.

Cryptocurrency and Defined Contribution Plans

Cryptocurrency ("crypto") has become popular in the marketplace and the financial press, but this does not mean it is suitable for retirement plans. That is the position taken by the Department of Labor (DOL) in their recent guidance and additional communications aimed at plan sponsors. Compliance Assistance Release No. 2022-01 identifies several concerns regarding crypto that involve the fiduciary responsibilities of plan sponsors. Additionally, the DOL stated that they expect to conduct investigations of plans that offer crypto.

When selecting investments, fiduciary duties include the following:

1. Using a framework, such as an Investment Policy Statement (IPS)

2. Gathering relevant quantitative and qualitative information

3. Determining if the investment complies with IPS criteria

4. Making the decision to either include it in the menu or not

5. Documenting the process used as well as the ongoing review of the investment if it included in the plan menu

With respect to crypto, the DOL advises plan sponsors to "exercise extreme care." Plan sponsors are urged to consider how crypto aligns with their responsibilities to exercise prudence with respect to investments, as well as their duty of loyalty to participants. In a move that surprised some, the DOL stated this evaluation also applied to including crypto in a brokerage window and that this was not a "novel" position because of the specific concerns surrounding this type of investment.

(continued on the next page)

Cryptocurrency and Defined Contribution Plans

The DOL cited 5 current concerns with respect to why crypto is likely not suitable for retirement investment menus. They include the following:

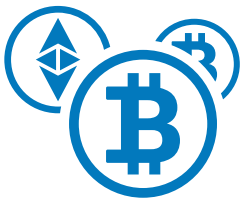
1. Crypto has "been subject to extreme price volatility."

2. Crypto might appeal to the unsophisticated investor and appear to be deemed prudent by those overseeing the plan.

3. Crypto presents custodial and recordkeeping concerns.

4. Crypto presents difficulties with reliable valuation.

5. The regulations governing crypto are evolving.



The steps below are for plan sponsors who want to learn more about the DOL's current position on crypto, are considering adding it to their plans, or in those rare circumstances that have already added it:

1. Review the DOL Compliance Assistance Release and other relevant communications.

2. If you have not added crypto, develop a communication strategy for participants who request it.

3. Continue to monitor regulatory developments concerning crypto.

4. If you have added crypto, review the process used to determine if it was prudent to do so and seek input from ERISA counsel competent to advise you in this highly specialized area.

In light of the DOL's compliance assistance, NWCM recently published the a memo as a resource to plan sponsors in the event they receive questions regarding adding crypto investments to their defined contribution retirement plans. Additionally, an interview conducted with the Employee Benefits Security Administration's (EBSA) Tim Hauser provides additional rationale on the DOL's compliance assistance. If you would like to know more, please contact an NWCM advisor.

RECENT ERISA LITIGATION

Hughes v. Northwestern University – Excessive Fee Case

Case Summary: In December 2021, the Supreme Court reviewed a case regarding an allegation of excessive plan fees and imprudent plan investment options. The plaintiffs in the case alleged that the plan had breached their duty of prudence under ERISA by (1) failing to include the lowest-cost share class of a fund; (2) including too many investment options in a plan thereby causing participant confusion; and (3) allowing plan recordkeepers to charge excessive fees. The Seventh Circuit dismissed the case, finding that the plaintiffs had not made sufficient allegations and therefore should not be allowed to proceed to trial. The plaintiffs petitioned the case to the Supreme Court to assess whether or not the allegations were sufficient under ERISA to proceed to trial.

Case Update: In a unanimous decision, the Supreme court vacated the Seventh Circuit's decision, remanding the case back to the Seventh Circuit to re-evaluate the allegations as a whole, and consider whether the plaintiffs plausibly alleged a breach of duty. The decision makes an important distinction, noting that the inclusion of an "adequate array of investment choices," including lower cost options, does not excuse the inclusion of imprudent investment options. Thus, plan fiduciaries must monitor all investments included in the plan's menu and remove any imprudent investments from the plan within a reasonable amount of time. The decision overall was narrow, with the Supreme Court stating that such claims should be scrutinized on a context-specific, case-by-case basis.

It is important to note that the Supreme Court was not ruling on the merits of the case, and thus they issued no opinion on the factual basis of any of the allegations made. Their role was only to determine whether the claims noted above, on their face, established enough legal cause of action to be reconsidered or whether the lower court's dismissal should stand. Although they ruled in favor of the plaintiffs, the Supreme Court acknowledged in their decision that "the circumstances facing an ERISA fiduciary will implicate difficult tradeoffs, and courts must give due regard to the range of reasonable judgments a fiduciary may make based on her experience and expertise."

Action Item: The decision in this case emphasizes the importance of properly monitoring all investments, removing imprudent ones within a reasonable time, and ensuring the reasonableness of plan fees. Fiduciaries should document their decisions and the basis for those decisions, as the duty of prudence focuses on the process for making fiduciary decisions.

RECENT ERISA LITIGATION

Smith v. GreatBanc Trust Co., Smith v. Board of Dirs. of Triad Mfg., Inc., – Mandatory Arbitration Case

Case Summary: Whether mandatory arbitration provisions in ERISA plan documents are enforceable.

Case Update: In 2020, it was ruled in Smith v. GreatBanc Trust Co. that a mandatory arbitration was unenforceable because the plaintiff had not received notice that the plan had been amended to include the provision. The case was appealed to the Seventh Circuit in 2021. The Seventh Circuit affirmed the previous decision, denying the motion to require mandatory arbitration in this case.

The enforceability of mandatory arbitration provisions under ERISA remains an unsettled area of law. Recent decisions in the Seventh Circuit, as well as state district courts have reached conflicting results, and courts of appeals remain split on key issues concerning the scope and application of these provisions. Until the Supreme Court agrees to hear a case on mandatory arbitration, plan sponsors and plan fiduciaries will continue to face uncertainty.

Congress has continued to show interest in bills relating to mandatory arbitration clauses. On March 17, 2022, the House narrowly passed legislation known as the Forced Arbitration Injustice Repeal (FAIR) Act. The bill would void pre-dispute mandatory arbitration agreements in employee benefit plans. The White House has endorsed the bill; however, given its scope, the bill's outlook is uncertain. If passed, the law would not apply retroactively and so any existing arbitration agreements would not necessarily be invalidated.

Action Item: Plan sponsors and plan fiduciaries should consult legal counsel when considering adding a mandatory arbitration provision to their plan document.

Giannini v. TransAmerica Retirement Solutions, LLC. – Cybersecurity

Case Summary: In a class action lawsuit filed in late 2021, plan participants alleged that their plan administrator, TransAmerica, failed to safeguard participant data resulting in a data breach. According to the complaint, unauthorized parties were able to gain access to participant data (including names, addresses, Social Security Numbers, and retirement fund contribution amounts) due to a lapse in network security. The plaintiffs also allege that Transamerica failed to notify participants of the breach in a timely manner. TransAmerica has responded that the allegations in the lawsuit are inaccurate and misleading, and they deny that they failed to meet any legal or regulatory obligations.

Action Item: While the outcome of this complaint is still pending in the courts, it is clear that cybersecurity related incidents involving retirement plans are on the rise. As noted in the recent cybersecurity guidance published by the DOL, responsible plan fiduciaries have an obligation to ensure the proper mitigation of cybersecurity risks. The DOL's cybersecurity guidance is "sub-regulatory", as opposed to formal regulation; however, this guidance has the potential to impact future ERISA litigation. Plan sponsors and fiduciaries should keep this guidance in mind when selecting and monitoring plan service providers in order to ensure the security of participant data.

RECENT ERISA LITIGATION

Jones et al. v. DISH Network Corporation et al. – Actively Managed Target Date Funds Case

Case Summary: In a class action lawsuit filed in early 2022, plan participants allege that the Dish Network Corporation 401(k) Plan committee breached their fiduciary duty by selecting and retaining the Fidelity Freedom target date funds (TDFs). According to the plaintiffs, the actively managed target date suite was "riskier and more costly" than alternative target date options and that the committee failed to compare the merits and features of the Fidelity Freedom funds to other available TDFs.

Although not a defendant in the lawsuit, Fidelity has filed an amicus brief on behalf of the plan sponsor, asserting that the actively managed Freedom Funds are a sound and proven investment choice for retirement plans. In their brief, Fidelity notes that actively managed funds tend to charge higher fees as they require extensive due diligence and research, which may potentially add value to performance. Fidelity notes that courts have previously rejected the notion that actively managed strategies are inherently imprudent. Fidelity also argued that the complaint failed to allege any concrete facts to demonstrate that the Freedom Funds were overly risky.

Action Item: This case, regardless of its merits, emphasizes the importance of following a prudent investment selection process.

Active and passive management are two different approaches to investing with different aims, risks, and potential performance outcomes. In exchange for typically higher fees, active management provides an opportunity to obtain market-beating returns, while lower-cost index funds track the performance of market indexes and go up or down based on market conditions. Either approach, or a mix of the two, may be used as long as there is a prudent process in place.

NWCM Fiduciary Focus Contributors

Nicholas Axline, QKA - Retirement Plan Service Associate
nicholasa@nwcm.com

Valerie Haley, QKA - Retirement Plan Service Associate
valerieh@nwcm.com

Thomas Resner - Director of Retirement Plan Operations
thomasr@nwcm.com

Guest Contributors

Chris Martin - Sr. Investment Advisor
Northwest Capital Management

Bonnie Treichel - Chief Solutions Officer
Endeavor Retirement

Helpful Resources

https://carsongroup.wistia.com/medias/zwg3s60vo1
NWCM's Plan Sponsor Best Practices Video on Cybersecurity

https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414
Department of Labor Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries Recordkeepers, Plan Participants*

*By clicking the above link, you will be leaving this website. The linked third-party information being provided through this page is strictly as a courtesy. NWCM is not liable for any direct or indirect technical or system issues or any consequences arising out of your access to, or your use of third-party technologies, websites, information, and programs made available through third-party websites. You assume total responsibility and risk for your use of these third-party websites