NWCM FIDUCIARY FOCUS

EDITION 2 - 2021

A summary of key fiduciary takeaways for Plan Sponsors

RETIREMENT FIDUCIARY AND REGULATORY COMPLIANCE

REPORT BY NWCM PLAN DEPARTMENT
OCTOBER 2021

FOR PLAN SPONSORS

The Olympic Mountains
Located along the Olympic Peninsula

TABLE OF CONTENTS

The information summarized may vary based on plan type and may be subject to adjustment due to changes in applicable state and federal laws. The information is offered as general guidance only and is not to be relied on as specific legal advice. For legal advice on a specific matter, please consult with an attorney.

A NOTE FROM THE NWCM TEAM

Welcome to Northwest Capital Management's second edition of the Fiduciary Focus! As the days get shorter and the air cooler, there is much to look forward to with changing fall colors and the holiday season spent with family and friends. Things less welcome are the threats posed by cyber-attacks on retirement plans. As you know, these malicious attacks pose a very serious problem for both plan sponsors and participants. SolarWinds, Colonial Pipeline and other high-profile incidents have left many feeling vulnerable in totally new ways. It seems plan sponsors are greeted with headlining cybersecurity threats so often that the word "warning" has been worn out.

Fortunately, the Department of Labor (DOL) has published a set of guidelines intended to alert fiduciaries to growing cyber-threats and ways to address them. While some practitioners may question the depth of these guidelines, the issues of cybersecurity are too great for the regulators to avoid or ignore. The DOL felt they had to start somewhere.

We at NWCM see these guidelines as another step in a continuing effort to develop 21st Century responses to current and developing threats to retirement security.

In this issue of the Fiduciary Focus, the main article provides an overview of the three sets of guidelines issued by the DOL. Additionally, we provide links to several resources designed to help plan sponsors learn about and prepare for a more robust plan data security environment.

We hope you find these resources valuable and look forward to your feedback and comments about what you would like to see in future publications.

FIDUCIARY TIP:
CYBERSECURITY WEBINARS

NWCM offers webinars and on-demand videos designed specifically for plan fiduciaries. The videos below provide insight and resources to help guide you towards developing a compliant cybersecurity program.

Cybersecurity Threats: Insights and Strategies to Help Protect Your Retirement Plan

Retirement Plan Service Agreements: A Focus on Cybersecurity

Deborah Fabricant and Boutwell Fay LLP are not affiliated with NWCM and opinions expressed by the presenter may not be representative of NWCM.

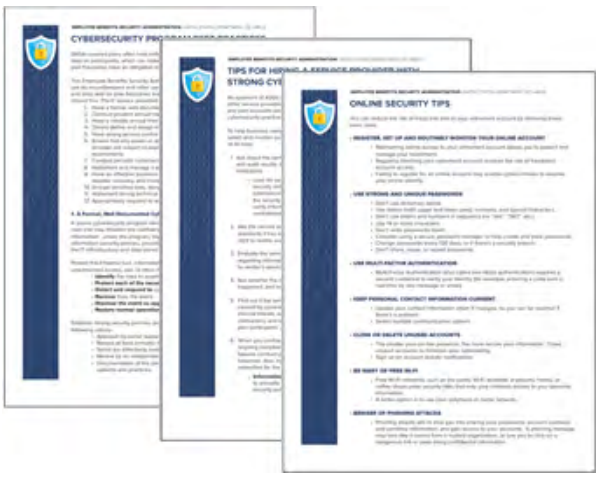
CYBERSECURITY: AN EMERGING FIDUCIARY CHALLENGE

Summary:

The Department of Labor (DOL) recently released **cybersecurity guidance** for plan sponsors to address the recent questions, issues, and lawsuits surrounding cybersecurity.

The three pieces are linked below:

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



In our main article below, the NWCM team takes a detailed look at why the DOL's guidance was released and what plan sponsors need to know about their fiduciary responsibility with regards to cybersecurity.

CYBERSECURITY: AN EMERGING FIDUCIARY CHALLENGE

While cyber-attacks like the one on the Colonial Pipeline make headlines, a more subtle and personally threatening form of cybercrime has been on the rise. These events involve the hacking of retirement plans and the participant accounts contained within them. The number of cases has been relatively small so far.[1] However, these incidents have generated considerable legal activity and interest on the part of retirement plan professionals and regulators. Any threat to the integrity of retirement accounts rings alarm bells and for good reason. No individual suffering a loss of retirement savings due to a cyber-attack would think of this as a "small problem."

In an effort to bring attention to the issue, the Department of Labor (DOL) issued a set of guidelines intended to both provide information on and assist with the developing cybersecurity threat. While retirement practitioners are split on the efficacy of these guidelines, plan sponsors, practitioners, and regulators are in agreement that this issue cannot be ignored.[2,3]

The DOL's method is neither law nor regulation. It instead provides three sets of recommendations to address cybersecurity in relation to different target groups or activities. They include the following:

- **Cybersecurity Program Best Practices** - Recommendations for plan sponsors on how to build, test, and maintain a robust cybersecurity program for their retirement plan(s)
- **Tips for Hiring a Service Provider** - Recommendations for plan sponsors who are planning for or in the process of selecting new plan service providers
- **Online Security Tips** - Recommendations for plan sponsors on how to improve cybersecurity awareness and conduct for their plan participants

Each list, particularly the Online Security Tips, reads like a common sense set of recommendations, but as one might expect, one person's reasonable suggestion might become another's confounding dilemma. In an effort to assist our plan sponsor clients in making sense of the guidelines, we are offering suggestions on the process of improving data security and finding resources that will help with this effort.

Guidance 1: Cybersecurity Program Best Practices

This DOL guidance is focused on providing plan sponsors instructions on how to build, test, and maintain a robust cybersecurity program for their retirement plan(s). Thus, **plan sponsors must develop a cybersecurity program and make this program a priority element of the plan governance process.** Fortunately, many firms are already quite serious about cybersecurity when it comes to their business.

We recommend that the retirement plan committee process benefit from the same kind of attention. The DOL lists these six elements of a robust cybersecurity program:

- **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.

This guidance is further expanded upon in the **DOL's guidance**.

If your business lacks cybersecurity infrastructure, take advantage of the sources of assistance available to businesses. Many are sponsored by industry groups or governmental agencies and are cost-free sources of key information.[4]

Identify all of the service providers that interact with your retirement plan and ask each to detail their cybersecurity protocols and any elements concerning cybersecurity in their service agreements and have all such service agreements reviewed by Employee Retirement Income Security Act (ERISA) counsel with expertise in the Prohibited Transaction Exemptions concerning such service agreements.[5]

It is also paramount, per DOL guidance, that plan sponsors document all of these steps.

Guidance 2: Tips for Hiring a Service Provider

This guidance provided by the DOL gives recommendations for plan sponsors on selecting third-party service providers, and once hired, monitoring their cybersecurity policies. A new relationship with a plan service provider offers a unique opportunity to get things started on the right foot in so many ways, cyber matters included. Given the developing nature of both the cyber threat and the appropriate response, the DOL placed particular emphasis on the due diligence that should be applied to new service provider relationships. The DOL's tips in this area include the following:

1. Asking service providers about their information security standards, practices and policies, and audit results, and comparing them to industry standards.
2. Asking service providers how it validates its practices, and what levels of security standards it has met and implemented.
3. Evaluating service providers track record in the industry.
4. Asking whether service providers has experienced past security breaches, what happened, and how the service provider responded.
5. Finding out if service providers carry insurance policies which would cover losses dealing with cybersecurity.
6. Making sure that a contract with a service provider requires ongoing compliance with cybersecurity and information security standards.

The above is further expanded upon in the **DOL's guidance**.

Clearly, the service agreement is a key subject of this due diligence process and calls for particular scrutiny by appropriately skilled and experienced professionals such as an ERISA attorney. This is because the indemnity elements of these agreements concerning cyber incidents may appear to offer protections but have significant gaps in their application.[6] In this case, indemnity is the contractual responsibility to compensate the loss incurred by a cybersecurity breach to the affected party.

As one would expect, this piece suggests that plan sponsors collect documentation concerning the service provider protocols and levels of data security the service provider has implemented. The tips piece also suggests that plan sponsors inquire about past data breaches experienced by the service provider and how they were remediated. This could prove problematic since breach incidents may not have been published and the remediation measures may need to be kept out of the public realm to be effective.

CYBERSECURITY: AN EMERGING FIDUCIARY CHALLENGE

Because cybersecurity issues are an evolving threat, plan service providers are scrambling to develop service agreements that are both reasonable and offer all parties sufficient protections. Careful due diligence is a must, as is documentation of all efforts made.

Guidance 3: Online Security Tips

This DOL guidance aims to give plan sponsors recommendations on how to improve cybersecurity awareness and conduct for their plan participants. According to research by IBM, 95% of security breaches can be traced back to human error.[7] When it comes to retirement plan breaches, plan participants are often both the target and the weakest link.[8] The magnitude of this challenge cannot be overstated. Regardless of the reminders about not sharing passwords or having them written on sticky notes attached to computers, participants will fall victim to the increasingly sophisticated methods of experienced hackers. The DOL's guidance for plan participants includes the following:

- Register, set up, and routinely monitor your online account
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Close or delete unused accounts
- Be wary of free Wi-Fi
- Beware of phishing attacks
- Use antivirus software and keep apps and software current
- Know how to report identity theft and cybersecurity incidents

These tips are expanded upon in the **DOL's guidance**.

IT professionals working for IT-centric firms have developed ways of uncovering lapses within their own employee groups, often pretending to be hackers themselves. These methods can help identify employees that may require additional training. No amount of preparation or training can completely prevent cybercrime. Because the threat keeps evolving, so must the efforts to defend crucial data. This is another area where reference material on industry and association best practices comes in to play. The footnotes contain a number of useful reference sources.

In the case of fiduciary process, the key element of a good defense against accusations of fiduciary breach is to make and document continuous efforts at teaching the art of data security.

Conclusion

As with most evolving challenges, the response must attempt to keep pace with the threat. Our recommendation is for plan fiduciaries to commit to investing the necessary resources for maintaining a robust data security program. This includes assigning someone within the group to lead the effort, including this person in the ongoing committee meeting process, having outside experts periodically evaluate the program you develop, and documenting your actions every step of the way.

With this guidance, the DOL has attempted to provide much needed clarity on how to protect the data and retirement savings of plan participants, but this can be overwhelming for plan sponsors who have more going on than handling the cybersecurity of their employees' retirement accounts. **Because of this, NWCM will publish a detailed checklist later this year giving actionable items to plan sponsors to ensure they are following cybersecurity best practices. If you have any questions, please reach out to your NWCM advisor. We are always here to help.**

RECENT ERISA LITIGATION

1

Hughes v. Northwestern University – Excessive Fee Case

Summary: In July, the Supreme Court agreed to review a case related to excessive plan fees.

The plaintiffs in the case allege that Northwestern University breached their duty of prudence under ERISA by (1) paying excessive recordkeeping fees (by using multiple recordkeepers and allowing recordkeeping fees to be paid through revenue sharing) and by (2) offering mutual funds with excessive fees.

This will be the first time the Supreme Court addresses whether it is a breach of duty if a retirement plan paid or charged its participants fees that substantially exceeded fees for alternative available investment products or services.

2

Smith v. GreatBanc Trust Co. – Mandatory Arbitration

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

Update: On February 11, 2021, the House reintroduced legislation known as the Forced Arbitration Injustice Repeal (FAIR) Act. The FAIR Act would ban mandatory arbitration agreements and, if enacted, would apply to employee benefit plans. President Biden has indicated he would support signing the bill into law if passed by Congress.

RECENT ERISA LITIGATION

Bartnett v. Abbott Labs – Cybersecurity

3

Summary: Whether a Plan Sponsor's fiduciary responsibility makes them liable in the event of a recordkeeper/third-party vendor cybersecurity breach.

Update: In April, the Department of Labor (DOL) released cybersecurity guidance for plan fiduciaries. Barnett v. Abbott Laboratories provided a clear example of the importance of ensuring the cybersecurity of retirement plan data, which is reflected in the DOL's renewed interest in the area. The DOL guidance provides tips for Plan fiduciaries to select service providers that follow strong cybersecurity practices.

Harmon et al. v. Shell Oil Co. – Participant Data

4

Summary: Whether plan data counts as a "plan asset" under ERISA.

Update: In March, a District Judge for the United States District Court for the Southern District of Texas granted Fidelity's motion to dismiss the case. In the ruling, the court determined that participant data does not meet the statutory definition of "plan assets" under ERISA.

The decision was made following a review of DOL's regulations defining "plan assets", as well as a review of recent rulings that came to a similar conclusion. ERISA itself does not clearly define what constitutes a "plan asset", but regulation issued by the DOL primarily discusses plan assets with regards to investments. So far, no court has extended the definition of plan assets to include participant data. However, this issue may be appealed to higher courts or may continue to be brought forward in lower courts.

For now, fiduciaries can attempt to place restrictions on the use of participant data when negotiating vendor service agreements. Fiduciaries should also review their current service agreements to confirm what their vendors stance is on the use of participant data for purposes outside plan administration.

NWCM Fiduciary Focus Contributors:

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

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

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

Helpful Resources:

1. **https://www.sans.org/**
   The SANS Institute is a trusted resource for cybersecurity training, certifications and research.*
2. **https://www.isaca.org/resources**
   ISACA (the Information Systems Audit and Control Association) offers a variety of training options from knowledge-based to practical training and credentialing.*
3. **https://www.educause.edu/**
   Through the EDUCAUSE Cybersecurity Program, you can find the tools, resources, and peer connections
4. **https://www.sparkinstitute.org/**
   Free resources to help plan sponsors reduce exposure to various threats, learn about industry best practices, and get information*

*By clicking any of the above links, 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.

References:

[1] *So far, the number of incidents is dwarfed by other Significant Cyber Incidents, defined by the Center for Strategic and International Studies as attacks on government agencies, defense or technology companies, or involving economic losses in excess of $1 million. A list of such events kept since 2006 runs to 62 pages! But this differential offers little comfort to plan fiduciaries.*

[2] Moore, R. (2021, May 21). The DOL's CYBERSECURITY guidance in practice. PLANSPONSOR. https://www.plansponsor.com/dols-cybersecurity-guidance-practice/

[3] Rasmussen, M. (2021, April 27). DOL's new CYBERSECURITY GUIDANCE. JD Supra. https://www.jdsupra.com/legalnews/dol-s-new-cybersecurity-guidance-2460099/

[4] *The National Institute of Standards and Technology's Cybersecurity Framework is a set of guidelines for private sector companies to follow to be better prepared in identifying, detecting, and responding to cyber-attacks.* https://www.nist.gov/

[5] *A separate category of Prohibited Transaction Exemptions applies specifically to Service Agreements relating to benefit programs under ERISA.*

[6] *The indemnification clauses may appear to protect the plan sponsor from losses due to cyber-incidents, but may require steps on the part of the plan sponsors or their participants that are either impractical or unreasonably difficult to implement.*

[7] IBM Global Technology Services (2014). IBM Security Services Cyber Security Intelligence Index.https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

[8] Griffin, C. & Scott T Fisher. (2021, June 6). Cybersecurity Threats: Insights and Strategies to Help Protect Your Retirement Plan [Webinar]. Voya & Northwest Capital Management, Inc. https://carsongroup.wistia.com/medias/9g8rwknkip