Morgan Lewis

TECHNOLOGY MAY-RATHON

UNDERSTANDING THE PRACTICAL IMPACT OF THE DOL'S NEW CYBERSECURITY GUIDANCE

Elizabeth Goldberg, Matthew Hawes, and Michael Gorman

May 20, 2021

Presenters

Elizabeth S. Goldberg
Partner, Pittsburgh

Matthew H. Hawes
Partner, Pittsburgh

Michael J. Gorman
Associate, Washington, DC

Morgan Lewis

Introduction

- **20-Year Evolution of Increasing Electronic and Digital Reliance**
  - ERISA mandates that plan administrators must use delivery methods reasonably calculated to ensure actual receipt of information (29 C.F.R. § 2520.104(b)-1(b)(1))
    - Taxpayer Relief Act of 1997 – Directed the DOL to issue guidance on the use of new technologies by sponsors and administrators of retirement plans

- **1999 – DOL Proposed Safe Harbor**
- **2002 – DOL Final Safe Harbor (wired at work or consent)**
- **2006 – IRS Final Safe Harbor (effective access or consent)**
- **DOL FAB 2006-3 (pension benefit statements via continuous access website)**
- **DOL FAB 2008-03 (QDIA/ACA disclosures using DOL or IRS safe harbors)**
- **DOL Technical Release 2011-03R (enforcement policy regarding electronic delivery of investment disclsures)**
- **2019 – DOL Proposed New Safe Harbor**
- **2020 – DOL Final New Safe Harbor (email and other electronic communications)**

Introduction

- **20-Year Evolution of Increased Electronic and Digital Reliance**
  - 2019 – The DOL Proposed New Safe Harbor – allowing communication by email and smartphone
    - "The Department agrees that electronic delivery generally can be as effective as paper-based communication."
    - The DOL notes:
      - 87% of the US population lives in a home with broadband internet
      - 93% of households owning defined contribution accounts had used the internet in 2016
      - A 2015 survey of retirement plan participants indicated that 99% reported having internet access at home or work, and 88% reported having accessed the internet on a daily basis
      - Smartphones are used for more than just calling, texting, or basic internet browsing (e.g., a 2015 survey found that 57% of respondents had used a smartphone for online banking)

Increased Reliance on Electronic Communications with Participants and Online Account Access

- 2020 – New DOL Safe Harbor: "Default Electronic Disclosure by Employee Pension Benefit Plans under ERISA"

> *[The DOL] recognizes that increased electronic disclosures may expose covered participants' information to intentional or unintentional data breach … the Department expects that many plan administrators, or their service or investment providers, already have secure systems in place to protect covered individuals' personal information. Such systems should reduce covered individuals' exposure to data breaches.*
>
> * * * *
>
> ***[E]fforts to establish specific, technical requirements would be difficult to achieve, given the variety of technologies, software, and data used in the retirement plan marketplace**.*

LEGAL BACKGROUND

Cybersecurity Incidents Involving ERISA Plan Assets Are Happening and the Threat Is Likely to Increase

Increasing Theft in General

Cyberattacks are the fastest growing crime in the US with a global cost in excess of $6 trillion annually by 2021.

Increasing Incidents of Data Theft

Social Security theft, for example.

Increasing Reports of Theft from Plans, Example 1

Public report of plan participant's account being accessed in 2018 and 2019 and there was an unauthorized distribution of $245,000.

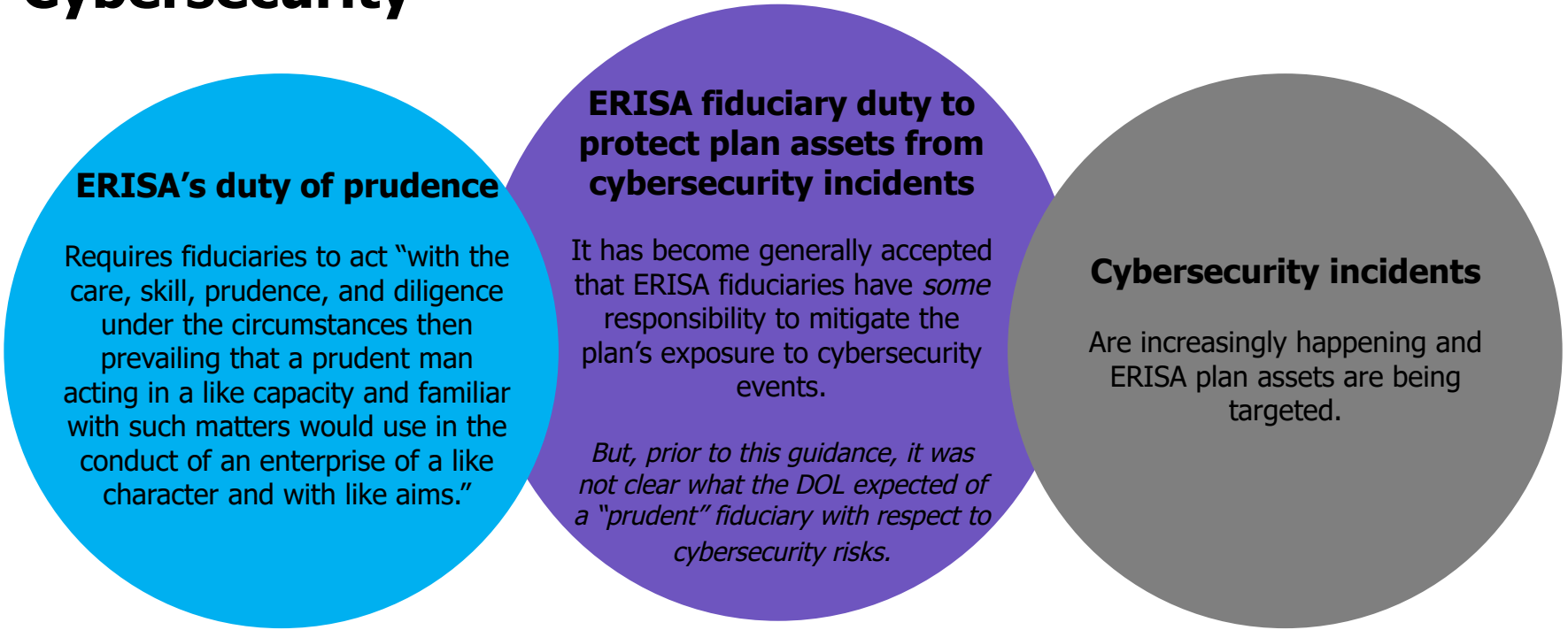
Increasing Reports of Theft from Plans, Example 2

Public report of $400,000 being taken from participant account in 2015 through fraud forms.

Increasing Reports of Theft from Plans, Example 3

Recent public report of $99,000 cybertheft of plan assets.

Nexus Between ERISA's Fiduciary Duties and Cybersecurity

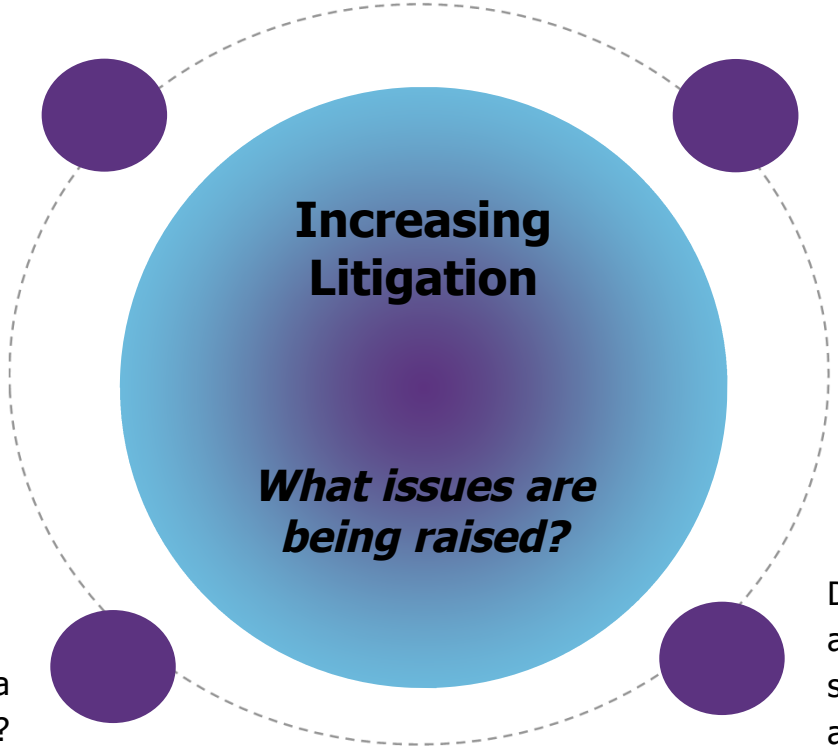


Litigation Background

- There has been increasing amounts of litigation over alleged identity theft and fraudulent distributions.
- Several lawsuits have been filed recently against plan sponsors, plan fiduciaries, administrators, and recordkeepers after thieves hacked plan participants' personal information and used that information to drain participants' 401(k) plan accounts.
  - Prior court precedent is relatively favorable to plan fiduciaries, but there is some concern that the law will become less favorable as additional cases (with worse facts) are heard.
- There has also been increased litigation alleging that plan fiduciaries have failed to properly secure plan data.

What Issues Have Been Raised in Litigation?

Was the plan sponsor, plan fiduciary, administrator, or recordkeeper acting as a plan fiduciary with respect to the acts that led to the theft from the participant's account?



How was the participant's data hacked? Was it through a plan-related source (such as the plan website) or an unrelated source (such as the participant's personal email)?

Is participant information a plan asset?

Does the complaint sufficiently allege that the acts of the plan sponsor, plan fiduciary, administrator, or recordkeeper actually caused the loss?

Significant Risks

- This area presents significant risks for plan fiduciaries
  - Retirement plans present an attractive opportunity for criminals to obtain the most sensitive of personal information
  - Plaintiffs' bar continues to be exceptionally active presenting novel theories of fiduciary liability
  - Proactive engagement of providers and security personnel and education and training
  - The DOL has telegraphed an upcoming enforcement initiative focusing on cyberliability issues
    - The DOL has criminal as well as civil investigatory authority

Reports Highlighting Cybersecurity Risks

- In November 2016, the ERISA Advisory Council published a report to the Secretary of Labor titled "Cybersecurity Considerations for Benefit Plans," which included questions regarding data protection that it thought may be helpful to plan fiduciaries contracting with and evaluating service providers.
- In March 2021, the GAO published a report examining the data that plan sponsors and their service providers exchange during the administration of defined contribution plans and the associated cybersecurity risks.
  - The report recommended that the DOL formally state whether it is an ERISA plan fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks in such plans.

DOL INTEREST AND NEW GUIDANCE

Morgan Lewis

There Are Many Signs the DOL Will Begin an Investigatory Initiative on Cybersecurity

Timothy Hauser, the DOL's Deputy Assistant Secretary for National Office Operations, has repeatedly commented on cybersecurity matters.

He has been quoted as stating that the DOL will be auditing retirement plans for cybersecurity and that the people responsible for plan administration should be paying attention to whether the systems are secure.

Julie Su, President Biden's nominee for the Deputy Secretary of Labor, has stated that cybersecurity will be an area of focus for the DOL.

Ali Khawar, the Acting Assistant Secretary for EBSA, has highlighted the DOL's cybersecurity efforts in recent speeches.

The DOL Issues First-of-Its-Kind Cybersecurity Guidance

- On April 14, 2021, the DOL issued three pieces of subregulatory guidance addressing the cybersecurity practices of retirement plan sponsors, their service providers, and plan participants respectively.
- Is the guidance enforceable?
  - While this subregulatory guidance is not entitled to deference—and arguably does not even have the persuasive authority of an Advisory Opinion—it provides a window into the DOL's expectations for a "prudent" plan fiduciary's cybersecurity practices.
  - For example, Ali Khawar is recently reported as characterizing the guidance as not establishing standards, but rather as outlining the best practices the DOL would like to see in terms of what each stakeholder group should be doing.

New Guidance

- Each of the three new pieces of guidance addresses a different audience.
  - *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* provides guidance for plan fiduciaries when hiring a service provider, such as a recordkeeper, trustee, or other provider that has access to a plan's nonpublic information.
  - *Cybersecurity Program Best Practices* is a collection of best practices for recordkeepers and other service providers, which may be viewed as a reference for plan fiduciaries when evaluating service providers' cybersecurity practices.
  - *Online Security Tips* contains online security advice for plan participants and beneficiaries.

ANALYSIS OF PLAN SPONSOR GUIDANCE

Morgan Lewis

Tips for Hiring a Service Provider

- *Tips for Hiring a Service Provider* outlines factors for "business owners and fiduciaries" to consider when selecting retirement plan service providers.
- While a plan fiduciary may have a variety of fiduciary obligations with respect to potential cybersecurity events, one of the most important responsibilities relates to properly ensuring that plan service providers have adequate safeguards to mitigate cybersecurity risks.
- This is because plan service providers normally have the most direct access to plan assets and are the most vulnerable to permitting fraudulent distributions.

Six Tips for Hiring a Service Provider

1. Ask about the service provider's data security standards, practices, policies, and audit results and benchmark those against industry standards.
2. Analyze the service provider's security standards and security validation practices.
3. Evaluate the service provider's track record in the industry.
4. Ask about past security events and responses.
5. Confirm that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity theft events.
6. Ensure that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

Tips for Hiring a Service Provider – Comments

- Conspicuously absent from this guidance is a clear statement regarding a fiduciary's obligations with respect to current service providers.
- Thus, fiduciaries may want to consider evaluating current agreements to better understand the service provider's obligations, sending questionnaires to service providers regarding their cybersecurity programs, and exercising audit rights.
- Plan fiduciaries could consider using the *Tips for Hiring a Service Provider* when preparing requests for information (RFI) and requests for proposal (RFP).
- When entering into a new agreement, the plan fiduciary could engage in meaningful negotiations over the terms of the agreement discussed in this guidance (e.g., cybersecurity, protection and use of confidential data, insurance coverage, etc.).

PROVIDER BEST PRACTICES

Morgan Lewis

Cybersecurity Best Practices

- *Cybersecurity Best Practices* is directed squarely at ERISA plan recordkeepers and other service providers who have access to plan-related IT systems and plan data.

- It summarizes 12 "best practices" that plan service providers "should" implement to mitigate exposure to cybersecurity risks. Although this guidance is specific to service providers, the DOL points out that plan fiduciaries should be aware of these best practices to enable them to prudently hire service providers.

- This implies that the DOL may take the position on audit that a plan fiduciary is being imprudent if they fail to ensure that the plan's service providers engage in these best practices.

12 Cybersecurity Best Practices

Practices 1–6

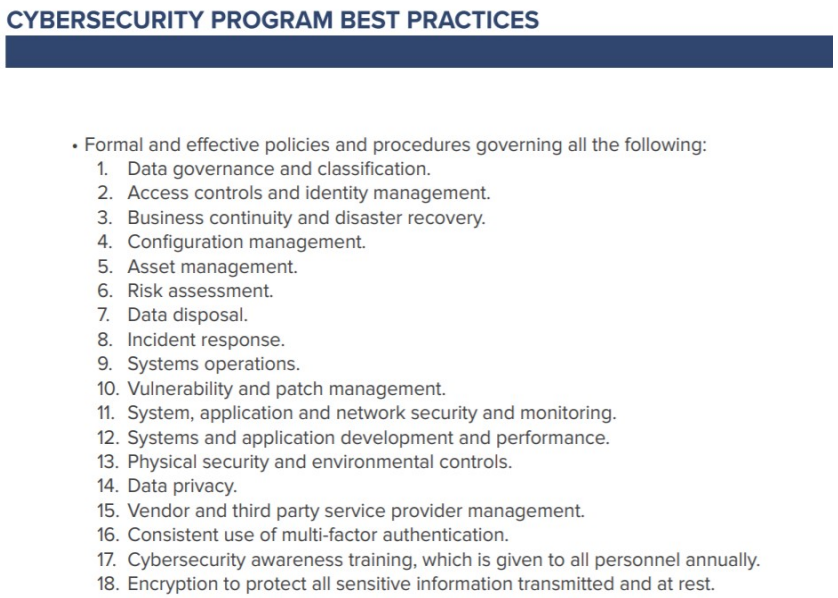
1. Have a formal well-documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access-control procedures
6. Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate safeguards

Practices 7–12

7. Conduct periodic cybersecurity training
8. Implement and manage an SDLC program
9. Have an effective business resiliency program addressing BCDR and incident response
10. Encrypt sensitive data, stored and in transit
11. Implement strong technical controls in accordance with best practices
12. Appropriately respond to any past cybersecurity incidents

Takeaways from the Cybersecurity Best Practices

- While these best practices can be summarized generally, the guidance itself includes significant detail on what the DOL will expect to see from a service provider that has implemented these best practices.
  - For example, the guidance identifies 18 areas that the formal cybersecurity program should address.



Takeaways from the Cybersecurity Best Practices

- Vendors may wish to consult with counsel and/or technical experts to determine how their current cybersecurity practices may be improved or otherwise better aligned with this guidance.

- Plan fiduciaries may wish to consult with counsel and/or technical experts to develop a strategy for documenting the process used to confirm that the plan's vendors are complying with this guidance.

PARTICIPANT GUIDANCE

Online Security Tips – Advice to Reduce Risk

Nine Tips for Participants

1. *Register, set up, and routinely monitor account*
2. *Use strong and unique passwords*
3. *Use multifactor authentication*
4. *Keep personal information current*
5. *Close or delete unused accounts*
6. *Be wary of free Wi-Fi*
7. *Beware of phishing attacks*
8. *Use antivirus software and keep apps and software current*
9. *Know how to report ID theft/incidents*

Administrator Considerations

- Encouraging participants and beneficiaries to follow these tips may help mitigate exposure to cybersecurity threats
  - Multiprong education campaign:
    - Window pop-ups
    - Emails and letters
    - Videos
    - SPDs

OPEN QUESTIONS AND CONSIDERATIONS

When Best Practices May Be More Than Best Practices

- While the DOL characterizes the guidance for fiduciaries and service providers as "tips" and "best practices," the language in the body of the guidance is stronger.
  - For example, *Tips for Hiring a Service Provider* states, "Plan Sponsors **should** use service providers that follow strong cybersecurity practices." (Emphasis added.)
  - Similarly, Cybersecurity Best Practices introduces a list of its 12 best practices as what "Plan's service providers **should**" do. (Emphasis added.)
- This distinction is particularly important given the DOL's repeated statements that it will start an enforcement initiative focusing on ERISA plan cybersecurity practices (and also the risk of plaintiffs' litigation continuing).
- We have seen the DOL treat "best practices" as required standards in other investigatory areas, namely the missing participant investigations.

Open Questions

- The DOL guidance issued on April 14, 2021 leaves open many questions. For example:
  - How should plan fiduciaries and service providers address existing arrangements that do not comport with the guidance?
  - Does the DOL believe that ERISA preempts state data privacy laws as they relate to ERISA benefit plans?
  - Does the DOL expect fiduciaries to communicate the *Online Security Tips* to participants and beneficiaries, and, if so, how often?
  - Which service providers does this cover?
  - For **plan sponsors**: what to do if the service provider will not adjust its program to meet the DOL's criteria
  - For **providers**: how to handle being responsive to the guidance and to plans seeking to implement the guidance, while also streamlining the program?

WHAT TO DO NOW?

What To Do Now?

Now May Be a Time for Plan Sponsors to Consider Proactive Steps

Basic Proactive Steps

- Review the guidance and consider the following steps.
- Consider a checklist evaluation that incorporates the DOL guidance.

Enhanced Proactive Steps

- Consider an enhanced self-assessment, such as:

✓ Review of select provider contracts and programs
✓ Conduct internal trainings (including fiduciary) on managing cybersecurity issues
✓ Review plan documents, including SPDs and participant communications
✓ Create a formal cybersecurity policy
✓ Educate participants

Highest-Level Proactive Steps

- Conduct a cybersecurity self-audit that replicates a DOL audit.
- *There may be value to engaging counsel in order to maintain privilege.*

Now May Be a Time for Providers to Consider Proactive Steps

Basic Proactive Steps

- Review the guidance and consider the following steps.

Enhanced Proactive Steps

- Consider an enhanced self-assessment, such as:

✓ Review of standard contracts and programs
✓ Conduct internal trainings (including fiduciary) on managing cybersecurity issues
✓ Create a formal cybersecurity policy

Highest-Level Proactive Steps

- Conduct a cybersecurity self-audit that replicates a DOL audit.
- *There may be value to engaging counsel in order to maintain privilege.*

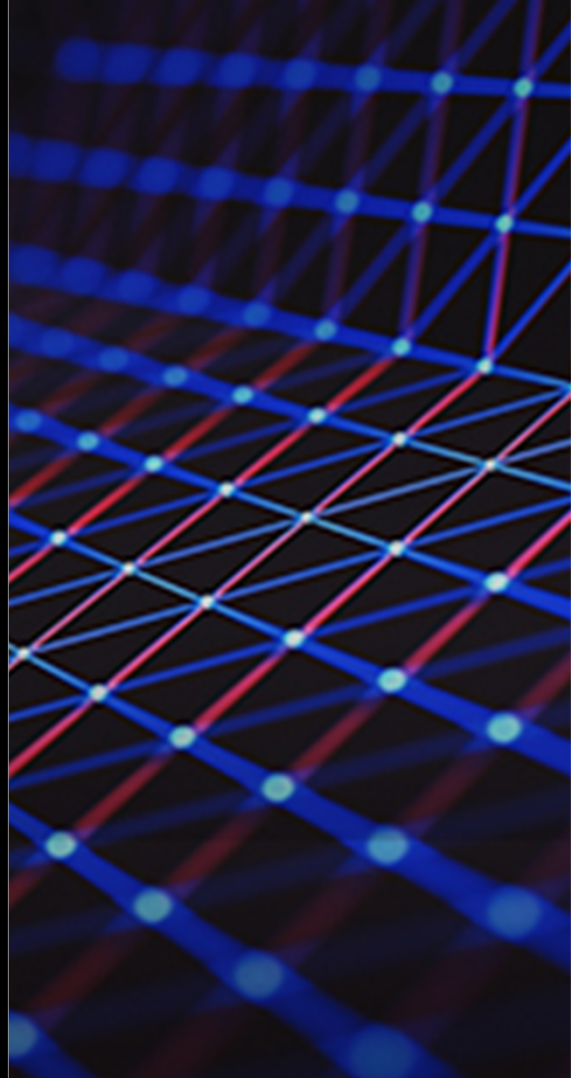

QUESTIONS?
Morgan Lewis

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.



Morgan Lewis

Biography

Elizabeth S. Goldberg
Pittsburgh
+1.412.560.7428
elizabeth.goldberg@morganlewis.com

Liz advises clients on ERISA matters with a focus on fiduciary responsibility provisions, prohibited transaction rules and exemptions, and the management of employee benefit plan assets. She negotiates investment-related agreements on behalf of plans and financial services providers; designs, implements, and administers employee benefit plans; and counsels clients on US Department of Labor (DOL) investigations, plan fiduciary governance structures, ERISA reporting and disclosure obligations, ERISA litigation, and general benefit plan compliance considerations. Liz's work experience includes several years at the DOL's Office of the Solicitor.

Biography

Matthew H. Hawes
Pittsburgh
+1.412.560.7740
matthew.hawes@morganlewis.com

Matt helps clients navigate every aspect of employee benefits, executive compensation, and equity compensation, including the drafting and design of qualified pension and profit-sharing plans, health and welfare arrangements, deferred compensation plans, and employee agreements, as well as compliance with reporting, fiduciary responsibility, and prohibited transaction requirements of the Internal Revenue Code (IRC) and ERISA.

Biography

Michael Gorman
Washington, DC
+1.202.739.5861
michael.gorman@morganlewis.com

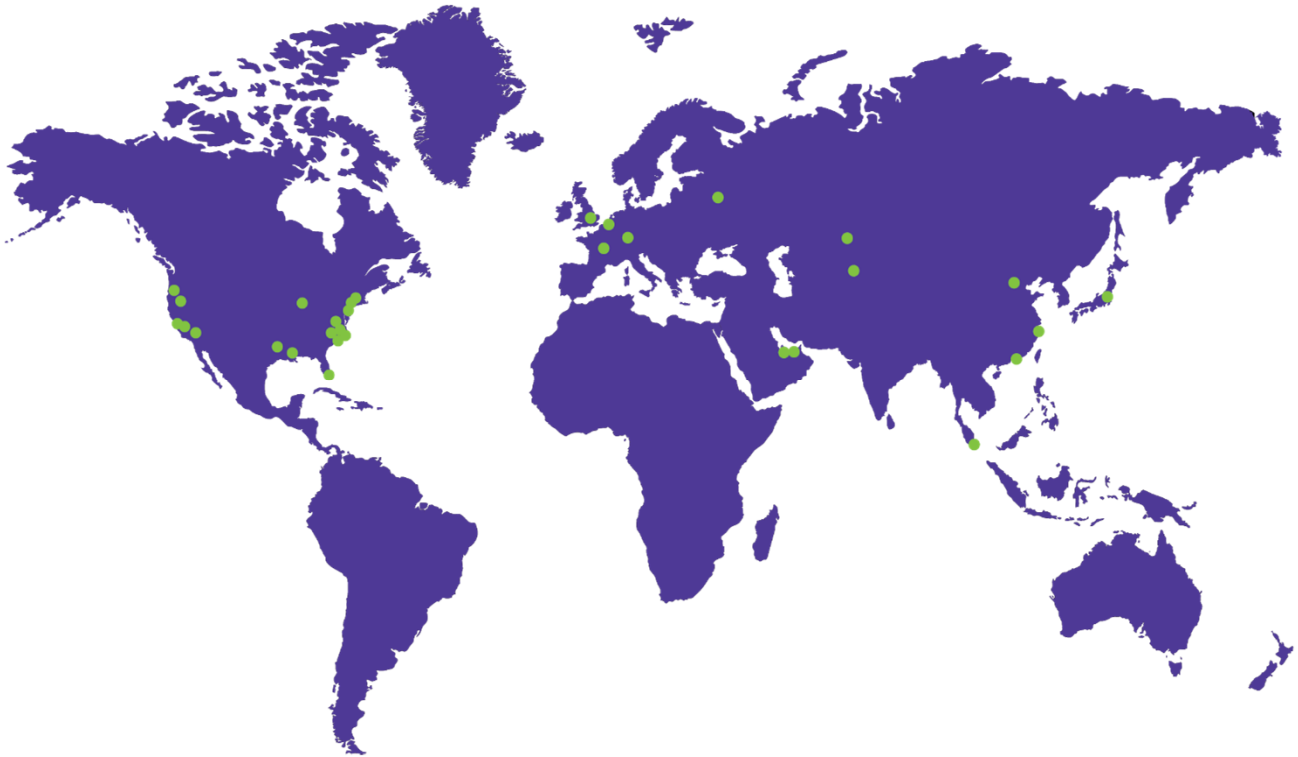
Mike advises multiemployer benefit funds, public and private companies, tax-exempt organizations, and governmental employers on the design, governance, operation, and compliance of qualified and nonqualified retirement plans and welfare benefit plans. Mike also counsels clients on legal issues arising under ERISA, the Internal Revenue Code, the Affordable Care Act, the Multiemployer Pension Protection Act, the Pension Protection Act, the Multiemployer Pension Reform Act, HIPAA, and COBRA. Prior to joining Morgan Lewis, Mike worked at a boutique law firm in Washington, DC, focusing on compliance issues confronting multiemployer plans.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.