Employee Benefits and Cybersecurity and Privacy Issues: 2022 Update

Morgan Lewis

Presenters

Matthew M. Hawes (Moderator)
Partner, Morgan Lewis

Sage Fattahian
Partner, Morgan Lewis

Elizabeth S. Goldberg
Partner, Morgan Lewis

Allison J. Fepelstein
Associate, Morgan Lewis

Michael J. Gorman
Associate, Morgan Lewis

Morgan Lewis

Introduction

Morgan Lewis

Legal Background on Cybersecurity and ERISA Plans

- ERISA's duty of prudence requires fiduciaries to act "with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims."
- It was generally accepted that ERISA fiduciaries have *some* responsibility to mitigate the plan's exposure to cybersecurity events. But, prior to the DOL's April 2021 guidance, it was not clear what the DOL expected of a "prudent" fiduciary with respect to cybersecurity risks.
- Cybersecurity events may implicate other fiduciary duties (e.g, loyalty) but the focus is on prudence.

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 US Department of Labor (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.

Cybersecurity Is a Priority for the DOL

- The Deputy Secretary of Labor, Julie Su, has stated that cybersecurity will be an area of focus for the DOL.
- Timothy Hauser, the Deputy Assistant Secretary for National Office Operations of the DOL, has repeatedly commented on cybersecurity matters.
  - "Plans hold lots and lots of money, and with lots of money there's lots of temptations for bad actors. . . . So far I think we've been fairly lucky in the plan universe. We have not had a huge catastrophic loss yet. But I do fear that may just be a matter of time."

DOL Focus Arises During Uptick in Private Litigation

- In the backdrop of this renewed DOL focus on cybersecurity is high-profile litigation over alleged identity theft and fraudulent distributions.
- 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.
  - The most prominent cases focus on whether the fiduciary had a prudent process and whether that process was followed.
- There has also been increased litigation alleging that plan fiduciaries have failed to properly secure plan data.
  - While this presentation focuses on the threat of identity theft and fraudulent distributions, cybersecurity events involving plan data are also a major concern.

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

- The DOL has repeatedly signaled that it would be turning its focus toward the intersection of cybersecurity practices and ERISA's fiduciary duties.
- 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.
- 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.

DOL 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 that 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.

Could Best Practices 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 Program Best Practices* introduces a list of its 12 best practices as guidance as to what a "Plan's service providers **should**" do (emphasis added).
- This distinction is particularly important, given the ongoing enforcement initiative focusing on ERISA plan cybersecurity practices.

The Role of Cybersecurity Professionals

- While legal counsel can assist plan fiduciaries in developing a prudent process consistent with the DOL guidance to monitor cybersecurity risks, lawyers may not be well situated to evaluate the strength of a vendor's cybersecurity practices.
- Thus, it may be appropriate for the plan fiduciary to engage a third-party cybersecurity vendor to evaluate the plan's vendors' cybersecurity practices.
  - To satisfy its duty of prudence, a fiduciary is not required to be an expert; however, the fiduciary may need to consult an expert.
- Plan fiduciaries and their third-party cybersecurity vendors (if any) may benefit from working hand in hand with the plan sponsor's IT professionals to develop a uniform response to cybersecurity threats.

Cybersecurity Concerns Extend Beyond Retirement Plans

- While the DOL guidance references protecting retirement benefits and pension plans, the focus of the guidance is on all ERISA-covered plan sponsors and fiduciaries, which presumably includes health and welfare plan sponsors and fiduciaries.
- Health and welfare plans are also subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).
- HIPAA and HITECH require group health plans to take measures to protect the privacy and security of protected health information (PHI).
  - PHI is individually identifiable health information that:
    - is created, received, or maintained by a group health plan or other "Covered Entity,"
    - relates to past, present, or future physical or mental health or condition or payment for provision of healthcare, and
    - identifies the individual directly or indirectly.
  - PHI includes oral, hardcopy, and electronic information.
  - Not all data is PHI. For example, enrollment information is not.

HIPAA and HITECH Compliance

- The US Department of Health and Human Services (HHS) published regulations under HIPAA/HITECH, including:
  - *Privacy Rule* – sets standards to limit how PHI is used and disclosed and to provide individuals with certain rights related to their PHI
  - *Security Rule* – defines administrative, physical and technical safeguards necessary to protect confidentiality, integrity and availability of electronic PHI (ePHI)
- The Office for Civil Rights (OCR) of HHS (not the DOL) is responsible for enforcing these rules.
- The DOL cybersecurity guidance is an added layer of compliance beyond the HIPAA/HITECH requirements.

Data Sharing

- In addition to the cybersecurity issues recently highlighted by the DOL, there are a number of thorny legal issues relating to the ability of plan sponsors and fiduciaries to share plan or participant data
  - Is plan data a plan asset?
  - Who must consent to sharing participant data?
  - Is it permissible for plan service providers to use participant data to sell participants non-plan services?
  - Disclosure issues
  - Opt in vs. opt out

The DOL's 2021 Cybersecurity 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.

More specifically, this guidance recommends steps that a plan fiduciary should take when hiring a service provider. These steps include the following:

Morgan Lewis

- Asking about the service provider's data-security standards, practices, policies, and audit results and benchmarking those against industry standards.

- Analyzing the service provider's security standards and security validation practices.

- Confirming that the agreement with the service provider permits the plan fiduciary to review cybersecurity compliance audit results.

- Evaluating the service provider's track record in the industry (e.g., security incidents, litigation).

- Asking about past security events and responses.

- Confirming that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity-theft events, including losses caused by internal threats (e.g., the service provider's employees) and external threats (e.g., third-party fraudulent access of participant accounts).

- Ensuring 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 – Commentary

- Conspicuously absent from this guidance is a clear statement regarding a fiduciary's obligations with respect to current service providers. However, it is reasonable to expect that the DOL may assert on audit that a plan fiduciary should have reevaluated its current service providers' practices and its current agreements in light of this guidance.
- 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. Depending on the terms of the agreement, a fiduciary may want to propose amending the services agreement to better align with the *Tips for Hiring a Service Provider*.
- 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 implicated in this guidance (e.g., cybersecurity, protection and use of confidential data, insurance coverage).

Cybersecurity Program Best Practices

- *Cybersecurity Program 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 make prudent decisions when hiring service providers.

- As discussed above, this implies that the DOL may take the position on audit that a plan fiduciary is being imprudent if it fails to ensure that the plan's service providers engage in these best practices. Arguably, the DOL could take this position with respect to service providers hired prior to the issuance of this guidance (and even with respect to services rendered prior to the issuance of this guidance).

Cybersecurity Program Best Practices (1-2)

The *Cybersecurity Program Best Practices* provide that:

1. service providers **should** have a formal, well-documented cybersecurity program that consists of policies and procedures designed to protect the infrastructure, information systems, and data from unauthorized access and other malicious acts by enabling the service provider to (1) identify the risks, (2) protect the assets, (3) detect and respond to cybersecurity events, (4) recover from cybersecurity events, (5) appropriately disclose the event, and (6) restore normal operations.
2. service providers **should** design and codify annual risk assessments that help identify, estimate, and prioritize risks to the information systems.

Cybersecurity Program Best Practices (3-4)

3. service providers **should** have a third-party auditor assess the service provider's security controls on an annual basis. The DOL indicated that as part of its review of an effective audit program, the DOL would expect to see, among other things, audit reports and audit files prepared and conducted in accordance with appropriate standards, penetration-test reports, and documented correction of any weaknesses.
4. service providers **should** clearly define and assign information security roles and responsibilities, with management of the cybersecurity program at the senior executive level and execution of the cybersecurity program by qualified personnel who have sufficient experience and certifications, undergo background checks, receive regular updates and training on current cybersecurity risks, and have current knowledge of changing threats and countermeasures.

Cybersecurity Program Best Practices (5-6)

5. service providers **should** have strong access-control procedures, including limiting access to authorized users; limiting access privileges based on role and the "need-to-access" principle; establishing a policy to review access privileges every three months; requiring unique, complex passwords; using multifactor authentication wherever possible; establishing policies, procedures, and controls to monitor authorized users and detect unauthorized access; establishing procedures to ensure that a participant's or beneficiary's sensitive information in the service provider's records matches the plan's information; and confirming the identity of authorized fund recipients.
6. service providers **should** ensure that any cloud or third-party managed storage system used by the service provider to service the plan is subject to proper security reviews and independent security assessments.

Cybersecurity Program Best Practices (7-8)

7. service providers **should** conduct periodic cybersecurity awareness training for all personnel pursuant to a comprehensive program that sets clear cybersecurity expectations and educates everyone to recognize sources of attack, help prevent incidents, and respond to threats.
   - The DOL emphasized identity theft—individuals posing as plan officials, fiduciaries, participants, or beneficiaries—as a leading cause of fraudulent distributions that should be considered a key topic of training.
8. service providers **should** implement and manage a secure "system development life cycle" (SDLC) program addressing both in-house developed applications and externally developed applications and that includes activities such as penetration testing, code review, and architecture analysis.

Cybersecurity Program Best Practices (9-10)

9. service providers **should** have an effective business resiliency program that addresses business continuity, disaster recovery, and incident response and allows for the organization to maintain continuous operations and safeguard people, assets, and data during periods of disruption.
10. service providers **should** implement current, prudent standards for the encryption of sensitive nonpublic information both while it is at rest and while in transit.

Cybersecurity Program Best Practices (11-12)

11. service providers **should** implement technical security controls consistent with best security practices, including hardware, software, and firmware that is kept up to date; firewalls and intrusion detection and prevention tools; current and updated antivirus software; routine patch management (preferably automated); network segregation; system hardening; and routine data backup (preferably automated).
12. service providers **should** respond appropriately to cybersecurity incidents that have occurred, including notifying law enforcement; notifying the appropriate insurer; investigating the incident; giving affected plans and participants information to prevent or mitigate harm; honoring contractual or legal obligations and fixing any problems in order to prevent recurrence.

Online Security Tips

- *Online Security Tips* recommends nine security tips for plan participants and beneficiaries as ways to better protect their online information and retirement accounts.
- These tips include using multifactor authentication, keeping contact information current, and avoiding phishing attacks.
- Plan fiduciaries may help mitigate the plan's exposure to cybersecurity threats by encouraging participants and beneficiaries to follow these tips.
- Plan fiduciaries may better satisfy their fiduciary duties, and better protect themselves in the event of a cybersecurity event, by emphasizing to participants the importance of following these tips.

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?
- Notwithstanding these unanswered questions, this guidance is a helpful starting place for ERISA plan fiduciaries trying to understand how their duty of prudence applies to the world of cybersecurity.

How to Respond to This Guidance

Morgan Lewis

Practical Steps to Respond to This Guidance

Review the guidance and consider working with service providers to ensure that existing data security protocols reflect the best practices set forth by the DOL.

Consider fiduciary training on how best to address fiduciary exposure to cybersecurity events.

Consider reviewing plan documents, including SPDs and participant communications.

- The cybersecurity world is rapidly evolving, and it may make sense to tweak plan provisions to better protect the plan, its fiduciaries, and participants.

Consider established formal procedures designed to ensure that cybersecurity issues are regularly considered and properly addressed.

Consider educating participants as to their obligations with respect to cybersecurity and advising them of the DOL's *Online Security Tips*.

Consider engaging counsel and third-party vendors to conduct a benefit plan cybersecurity audit to analyze potential weaknesses in cybersecurity practices and the best ways to resolve such weaknesses.

- There may be value to engaging third-party vendors through counsel in order to maintain privilege.

Vendor Questionnaires

- The DOL guidance asks that plan fiduciaries be aware of their vendors' cybersecurity practices, which may be essential to allow a plan fiduciary to fulfill its monitoring obligation.
- One way to gain an understanding of the vendors' cybersecurity practices is through the use of a questionnaire.
- The questionnaire would also enable a plan fiduciary to gather the context and historical information that the DOL highlights in the *Tips for Hiring a Service Provider*.

Vendor Agreements

- Another step that plan fiduciaries may wish to take is to have counsel review the relevant vendor agreements to ensure that the contract terms identified in the *Tips for Hiring a Service Provider* are included (or excluded) consistent with this guidance.
- This will also provide an opportunity for plan fiduciaries to seek representations and warranties from vendors as to their compliance with the *Cybersecurity Program Best Practices*.

DOL Cybersecurity Enforcement Initiative

Morgan Lewis

DOL Investigations

- Within weeks of issuing its cybersecurity guidance, the DOL began opening investigations into the cybersecurity practices of ERISA plan fiduciaries.
- These investigations often involved comprehensive information requests that were even more extensive than those summarized in the guidance.
- The DOL has informally signaled that these investigations are here to stay and that cybersecurity issues will be addressed in the vast majority of investigations.

Proactive Steps to Mitigating Audit Risk

- Given the level of DOL activity in this space, plan fiduciaries may wish to prepare for a DOL investigation into their approach to cybersecurity as an inevitability.
- Plan fiduciaries may wish to take significant steps in response to this guidance (e.g., hiring a third-party vendor to assist, preparing and adopting a cybersecurity policy statement, issuing a cybersecurity questionnaire to vendors, evaluating the terms of their vendor agreements).
- Properly documenting these steps could benefit the plan and its fiduciaries by creating a record of the steps that the plan fiduciary took to mitigate the plan's exposure to cybersecurity events and to facilitate compliance with the DOL guidance.

Cybersecurity Issues for Health & Welfare Plans

Morgan Lewis

Issues for Health and Welfare Plans

- Dispel the notion that the cybersecurity guidance does not apply to health and welfare plans because those plans have to comply with HIPAA/HITECH.
- Practical steps to consider in addition to HIPAA/HITECH obligations:
  - Consider working with service providers to ensure that existing data security protocols reflect the best practices set forth by the DOL, in addition to the HIPAA/HITECH requirements.
  - Consider educating participants as to their obligations with respect to cybersecurity and advising them of the DOL's *Online Security Tips*.
  - Address cybersecurity guidance when engaging with TPAs and as part of contracting, in addition to negotiating a Business Associate Agreement.
  - Consider documenting DOL cybersecurity compliance, either included as part of the plan's HIPAA Privacy and Security Policies and Procedures or separately.

Plan Data-Sharing Issues

Morgan Lewis

Data Sharing vs. Cybersecurity

- While cybersecurity and data-sharing issues overlap on a number of fronts, cybersecurity and data security are not synonymous.
- For example, a plan could have a robust cybersecurity program in place consistent with the DOL guidance but be engaged in data sharing that plaintiffs may argue is impermissible.
- There remains a number of open legal issues regarding the sharing of plan and participant data.

Data Sharing: Legal Risks

- ERISA Litigation Risks
  - Plaintiffs have filed cases alleging that plan fiduciaries breached their ERISA fiduciary duties by allowing recordkeepers/administrators to use plan data for cross-selling.
  - Plaintiffs allege that data used for cross-selling is a plan asset, and therefore the data must be used in the best interest of participants.
  - Cases include:
    - *Harmon v. Shell Oil Co., No.* 3:20-cv-00021 (S.D. Tex. Mar. 30, 2021)
    - *Divane v. Northwestern University,* 2018 US Dist. LEXIS 87645, (N.D. Ill. May 25, 2018), *aff'd,* 953 F.3d 980 (7th Cir. 2020), *rev'd on other grounds, Hughes v. Northwestern University,* No. 19-1401 (Jan. 24, 2022)
  - A number of settlements have been conditioned on limiting vendor use of data.

Data Sharing: Legal Risks

- Regulatory Risks: DOL
  - DOL's long-held position is that plan assets are determined based on ordinary notion of property rights.
    - If data is property of a participant (or plan), one would expect the DOL to view it as a plan asset.
  - DOL's recent guidance recommends addressing in the services agreement a vendor's obligations with respect to plan data.
  - DOL is currently prioritizing cybersecurity in investigations and has asked about the use of plan data by the plan vendor.
- Note that there are other possible areas of regulatory risk (e.g., SEC enforcement).

Data Still Not Viewed by Courts as a Plan Asset

- To date, no courts have found plan data to be a plan asset.
- This means that currently there is no judicial decision holding that the challenged practices breach ERISA.
- This leaves open (at least under ERISA case law) practices such as the following:
  - Maintaining participant data, including secondary data such as call-center notes and information regarding "triggering events";
  - Using information in a customer-interaction software program that is shared with affiliates;
  - Using participant data to solicit the purchase of non-plan retail financial products and services;
  - Deriving revenue from the use of data;
  - Soliciting products to plan participants; and
  - Not requiring opt-in or disclosure by plans or participants.

THANK YOU