Court Finds American Airlines Liable for Breach of Fiduciary Duty of Loyalty to its 401(k) Plans Because it Allowed BlackRock to Pursue ESG Objectives in its Proxy Voting

IN THIS ISSUE...

Court Finds American Airlines Liable for Breach of Fiduciary Duty of Loyalty to its 401(k) Plans Because it Allowed BlackRock to Pursue ESG Objectives in its Proxy Voting


Catherine L. Reagan |

Kim Ong

In *Spence v. American Airlines, Inc.*, after a four-day bench trial in the Northern District of Texas, U.S. District Court Judge O'Connor ruled that American Airlines breached its fiduciary duty of loyalty under the Employee Retirement Income Security Act of 1974 ("ERISA") by allowing BlackRock Institutional Trust Company, Inc. ("Blackrock"), as manager of all its passively managed non-ESG investments in American Airlines 401(k) plans, to use proxy voting policies to further environmental, social, and governance ("ESG") objectives. (*Spence v. Am. Airlines, Inc.*, No. 4:23-CV-00552-O, (Dkt. 157) (N.D. Tex. Jan. 10, 2025) (Findings of Fact and Conclusions of Law) ("*Am. Airlines II*").)

This case differs from the typical 401(k) plan "excessive fee" case where participants argue that an ERISA plan paid too much for investment management. On the contrary, here the district court acknowledged that American Airline's plans paid low rates for investment management fees, and focused instead on the relationship between American Airlines and BlackRock, and BlackRock's ESG policies for proxy voting. In an

unusual ruling, the Court found American Airlines acted prudently in selecting and maintaining BlackRock as its investment manager, but also found that it (counterintuitively) acted disloyally by allowing its own corporate interests to affect its fiduciary role in monitoring BlackRock.

Background

In *American Airlines*, a former pilot brought a class action lawsuit on behalf of 100,000 American Airline employees and pilots, accusing American Airlines and its Employee Benefits Committee ("EBC") of mismanaging their 401(k) plans by allowing BlackRock, as the investment manager, to pursue a "pervasive" ESG policy agenda through shareholder activism and proxy voting of shares that it holds by virtue of managing the plans' passively managed non-ESG funds.

The plaintiff argued that BlackRock had influence over American Airlines' decisions related to ESG because it managed approximately $11 billion of assets in their plans. At the same time, it was one of the largest owners (about 5%) of American Airlines stock and owned $400 million of American Airlines fixed income debt. BlackRock was also one of the largest owners of Aon Investments, USA ("Aon"), the company American Airlines hired to help monitor its plan investments and their managers _ including BlackRock. The district court referred to this as an "incestuous" relationship.

Understand that investment managers do not "own" shares of companies the way one would typically think of ownership; they manage investments for other investors, including but not limited to participants in various ERISA plans to which they provide services. However, because those investment managers are able to use proxies to vote the shares, they can use their significant voting power to impact company policy and, as was the case in a 2021 Exxon proxy vote, that can sometimes have an outcome determinative vote.

In the Exxon proxy vote, Engine No. 1, an activist and impact-focused investment firm, published a letter to Exxon's Board of Directors asking them to explore clean energy options. At a shareholder meeting, BlackRock voted for the Engine No. 1 dissident director candidates and three of them were elected to Exxon's Board of Directors. The district court noted that the three dissident directors would not have been elected but for BlackRock's votes in their favor. According to the plaintiff, shares in Exxon dropped after this vote, causing the American Airline plans damages (although the Exxon shares quickly rebounded).

Court Finds Breach of Fiduciary Duty of Loyalty, But Not of Duty of Prudence

In *American Airlines*, the district court was persuaded that BlackRock's influence caused American Airlines and the EBC to breach their ERISA fiduciary duty of loyalty, but not their fiduciary duty of prudence.

Duty of Prudence

Under the ERISA duty of prudence, a plan fiduciary must discharge its responsibilities using "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." (29 U.S.C. § 1104(a)(1)(B).)

The district court acknowledged that American Airlines and its EBC acted consistent with the prevailing industry standards for the duty of prudence, and in many ways actually "exceeded th[os]e standards." (*Am. Airlines, Inc.,* at pp. 47-52.) For example:

- EBC held quarterly meetings;

- EBC "hired a well-qualified advisor by engaging in a competitive process involving several leading investment firms, all of whom provided extensive information regarding their experience, resources, and manager-research procedures;"
- EBC received written and oral reports from that advisor quarterly; and
- American Airlines had internal investment professionals supplement external monitoring by independently meeting with investment managers, conducting independent due diligence, and reviewing and assessing quarterly reports before they went to the EBC.

The district court commented that the last step was "another layer of review that few large-plan fiduciaries replicate." It conceded that "there is no evidence that a prudent fiduciary adhering to its monitoring processes would have taken some action that Defendants did not with respect to BlackRock." The district court further acknowledged that most fiduciaries do not monitor proxy voting policies, and that the duty of prudence looks to what prudent fiduciaries would do in similar circumstances. Normally that would be the end of the analysis; however, the court found that this gold standard process could not protect American Airlines with respect to the duty of loyalty.

Duty of Loyalty

Under the duty of loyalty, an ERISA fiduciary must act "solely in the interest of the participants and beneficiaries and . . . for the exclusive purpose of (i) providing benefits to participants and their beneficiaries and (ii) defraying reasonable expenses of administering the plan." (29 U.S.C. § 1104(a)(1)(A).) The Supreme Court has interpreted "benefits" as used here to mean "financial benefits," not "nonpecuniary benefits." (*Fifth Third Bancorp v. Dudenhoeffer,* 573 U.S. 409, 421 (2014).)

The district court found "ERISA does not permit a fiduciary to pursue a non-pecuniary interest no matter how noble it might view the aim." The district court relied on emails American Airlines executives sent in a non-fiduciary capacity to find that the EBC and American Airlines allowed corporate policies and BlackRock to influence the management and oversight of the Plan. According to the district court, the defendants failed to take necessary precautions to separate their publicly stated corporate agenda of pursuing ESG objectives from their separate ERISA fiduciary duty to maintain the plan for the exclusive purpose of providing benefits to its participants and defraying expenses.

The district court found it significant that American Airlines "officials regularly discussed ESG in favorable terms without identifying the economic basis for such a view." It focused on communications among EBC members and American Airlines officials regarding BlackRock's publicly stated ESG investing policies, but noted there was no formal evaluation or assessment done by the EBC of those policies. When BlackRock expanded its proxy-voting choices to allow participants more control in how their proxy votes are cast, the EBC did not discuss BlackRock's new proxy voting options. The district court found the "absence of any internal analysis and monitoring of BlackRock's proxy voting to pursue ESG further suggests that Defendants took insufficient precautions [to] keep the corporate and fiduciary duties separate." The district court chastised American Airlines and the EBC for not closely monitoring plan proxy voting – something the district court acknowledges ERISA fiduciaries typically do not closely monitor. The district court found that, even though defendants use of BlackRock resulted in "comparatively lower fees," American Airlines and EBC acted disloyally as it relates to BlackRock's ESG investing because of their conflicting corporate and fiduciary interests.

The district court deferred its ruling on the issue of whether the plans suffered any damages, which has been fully briefed (but American Airlines has asked for leave to file a supplemental brief). If a judgment is issued, American Airlines may appeal the decision to the Fifth Circuit, but that circuit is generally not friendly to ESG policies.

The *American Airlines* decision comes a few months after the Fifth Circuit remanded *Utah v. Su* (109 F.4th 313, 322 (5th Cir. 2024)), a case challenging the DOL's ESG-friendly investment rule, back to the Northern District of Texas to reconsider in light of *Loper Bright Enterprises* (*Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024)), which overruled *Chevron* (*Chevron, U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 866 (1984), *overruled by Loper Bright*, 603 U.S. 369.)

On February 14, 2025, the Northern District of Texas district court upheld the ESG-friendly rule a second time, finding it is consistent with ERISA in saying that, between equal investment options, plan fiduciaries can choose "all valid options." (*Utah v. Micone,* No. 2:23-CV-016-Z, 2025 WL 510331, at *1 (N.D. Tex. Feb. 14, 2025).) The Fifth Circuit on its own directive took the court's order on appeal and requested briefing from the parties responding to the court's decision by April 25, 2025. With the change in administration, the DOL is unlikely to argue in favor of keeping the Biden-era ESG-friendly rule.

Final Comment

The American Airlines decision is a highly unusual ruling that finds a breach of the duty of loyalty but also holds that there was no breach of the duty of prudence. It remains to be seen whether this is an outlier decision that may be overturned on appeal or that may be applicable only in the Fifth Circuit if it is upheld. It seems unlikely to us that the case is the potential start of a larger trend. In any event, the case does provide a good primer on the procedural steps that a plan committee should follow to fulfill its duty of prudence regarding plan investments.

HHS Best Practices for ePHI Protection: What We Can Learn from the Proposed Modifications to the HIPAA Security Rule —Regardless of Whether It Becomes Final

Xiaolu Xu

In an effort to strengthen cybersecurity protections for electronic protected health information (ePHI), at the end of last year the Department of Health and Human Services (HHS) __ through its Office of Civil Rights (OCR) __ issued a Notice of Proposed Rulemaking (NPRM) to modify the Security Standards for the Protection of Electronic Protected Health Information ("Security Rule") under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act). The NPRM has received over 4,000 comments from HIPAA-regulated entities, healthcare industry stakeholders and the public. As discussed in this article, while it is unclear whether this proposed rule will be finalized (and if so, in what form), the NPRM contains helpful guidance for plan sponsors on what OCR considers to be best practices as it relates to the protection of ePHI.

Background

The HIPAA Security Rule, originally issued in 2003 and modified in 2013, adopted standards for the security of ePHI to be implemented by covered entities (i.e., health plans, health care clearinghouses and certain health care providers) and business associates (collectively, "regulated entities").[1] At a high level, the Security Rule requires regulated entities to implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of ePHI.

As the preamble to the NPRM notes, since the Security Rule's initial publication in 2003 and subsequent modification in 2013, the environment that regulated entities are operating in has undergone significant changes, and cybersecurity has become a critical concern affecting nearly every aspect of modern healthcare.[2] The preamble details a number of horror stories demonstrating the impact that cyberattacks can have on the healthcare industry and patient health. For example, in 2019 an Alabama hospital fell victim to a ransomware attack that disabled a large digital display, which likely contributed to the death of a newborn. In another example, a trauma center was hit by a ransomware attack that left it without access to electronic health records (EHRs) for 25 days. The attack affected 5,000 computers and destroyed the trauma center's electronic information systems that contained ePHI.

In response to these serious incidents and their consequences, OCR has also stepped up its enforcement on covered entities that fail to meet the Security Rule requirements. These investigations uncovered some covered entities' minimal or insufficient efforts to mitigate the risks to their ePHI.

Proposed Modifications to HIPAA Security Rule

Relying on the recommendations of the National Committee on Vital and Health Statistics (NCVHS), OCR's enforcement experience, news reports and the HHS' assessment of the environment, the 2024 NPRM proposes several significant changes to the existing Security Rule and discusses "best practices" contained in previously published guidance. The major proposed modifications which may impact group health plans, plan sponsors and their business associates are highlighted below. Due to the extensive nature of these changes, this article only provides an overview and does not contain a detailed description of each proposed change.

Revised and New Definitions

The NPRM proposes modifying the definition of "electronic media" to include not only data storage but also data maintenance and processing, reflecting the technologies now used by regulated entities for remote communication, such as communication applications on a smartphone or another computing device and messaging services that electronically store audio messages. This modification would also expand the definition to include future technologies, such as "any other form of digital memory or storage."

The NPRM also proposes adding ten new defined terms and modifying the definitions of fifteen existing terms to clarify how regulated entities should apply the standards and implementation specifications, and modernize the rule to better account for changes in the environment in which health care is provided.[3]

No Optional Implementation Specification

In the 2003 Security Rule the HHS introduced "addressable", as distinguished from "required," implementation specifications to give covered entities flexibility in deciding whether certain safeguards were necessary, based on factors such as risk and cost. However, in HHS's view some covered entities misinterpreted this, treating

compliance with "addressable" standards and specifications as optional. The NPRM would remove the distinction between "addressable" and "required," clarifying that regulated entities are required to implement all the standards and implementation specifications, and must adopt "reasonable and appropriate" security measures that allow the entity to achieve such implementation.

A required factor in determining whether a security measure is reasonable and appropriate is "the effectiveness of the security measures in supporting the resiliency of the regulated entity."[4] To reduce the impact that cyberattacks can have on the healthcare industry and patient health, information system resilience ensures that systems can operate under adverse conditions or stress – even in a degraded state – while maintaining essential functions and recover to effective operation status within a time frame consistent with mission needs.

Proposed Changes to Safeguards

Administrative Safeguards: The NPRM proposes adding explicit maintenance requirements to certain standards to address concerns that regulated entities may be misinterpreting the regulatory text regarding administrative safeguards, including:

- elevating the security management process to standard-level status
- requiring regulated entities to conduct a comprehensive written risk analysis of all ePHI
- mandating written assessments of changes impacting ePHI security
- requiring written policies and procedures for managing patches affecting ePHI
- elevating the risk management specification to address identified risks
- elevating the sanction policy specification to enforce consequences for non-compliance
- elevating the activity review specification covering all relevant electronic systems handling ePHI.

Physical Safeguards: The NPRM proposes to modify the existing standards that comprise the Security Rule's physical safeguards to clarify compliance obligations. The modification focuses on:

- clarify that physical safeguards apply to all ePHI within a regulated entity's facilities
- require written policies for controlling physical access to relevant systems and facilities
- ensuring that regulated entities properly consider physical safeguards for all workstations
- capturing various components of a regulated entity's electronic information systems that impact ePHI confidentiality, integrity, or availability.

Technical Safeguards: The NPRM proposes to modify the existing standards and implementation specifications to address the current failures to implement adequate technical controls or, in some cases, any technical controls. These proposed modifications include:

- clarifying that the requirement to implement and document technical safeguards applies to all technical safeguards
- requiring regulated entities to deploy technical controls in relevant electronic information systems to restrict access to authorized users and technology assets
- ensuring that any adopted encryption solution meets prevailing cryptographic standards before use
- requiring regulated entities to deploy technical controls that record and identify activity in their relevant electronic information systems and verify the identity of individuals or technology assets seeking access to ePHI.

Business Associate Agreements and Plan Documents – Contingency Plan

Under the existing Security Rule, a regulated entity must establish a contingency plan for responding to an emergency or other occurrence that damages systems that contain ePHI. The NPRM modifies this requirement by specifying the form and content of the contingency plan. A business associate would be required to report the activation of their contingency plan to the covered entity within 24 hours. A subcontractor of a business associate would also be required to notify such incidents to business associate. Furthermore, the NPRM requires this reporting obligation to be included in business associate agreements between covered entities and business associates, as well as in agreements between business associates and their subcontractors.The NPRM extends this obligation to plan sponsors, requiring that plan documents include language ensuring plan sponsors or their agents to implement Security Rule Safeguards for ePHI protection.

Written Verification from Business Associate

Under the existing Security Rule, a regulated entity must obtain written satisfactory assurances that its business associates will appropriately safeguard ePHI before allowing them to create, receive, maintain or transmit ePHI on its behalf. The NPRM requires further that a regulated entity verify its business associates' implementation of required *technical safeguards*. This includes obtaining annual written verification that business associate has deployed the technical safeguards, a cybersecurity analysis of business associate's electronic systems by a qualified professional, and a written certification from an authorized representative of business associate confirming the accuracy of the analysis. A covered entity would not be required to obtain such satisfactory assurances or verification from a business associate that is a subcontractor.

How the Security Rule would Apply to Artificial Intelligence (AI)

The preamble provides a brief discussion of the application of Security Rule with respect to the use of AI in medical devices and recognizes AI's enormous potential benefits. (The term AI is defined in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.) For example, the preamble notes that AI is being used in healthcare to summarize complex patient information from EHRs, aid in detecting conditions like diabetic retinopathy, and screen for cancer. However, as the preamble discusses, AI can also be used to harm individuals, both intentionally and unintentionally. For example, bad actors include using generative AI to threaten the privacy and security of ePHI more effectively through phishing and other social engineering.

The preamble clarifies that ePHI in AI training data, prediction models, and algorithm data that is maintained by a regulated entity for covered functions is covered by the Security Rule. Specifically, the preamble outlines the following expectations for a regulated entity using AI:

- Including AI tools in its risk analyses and risk management activities
- Performing a risk analysis to assess the impact of AI tools on the confidentiality, integrity, and availability of ePHI
- Including AI software that creates, receives, maintains, transmits, or interacts with ePHI, including when ePHI is used to train the AI, in the entity's technology asset inventory, which feeds into the risk analysis
- Monitoring authoritative sources for known vulnerabilities and remediate them according to its patch management program
- Ensuring patches, updates, and upgrades addressing critical and high risks are applied promptly.

The preamble also states that the adoption of the cybersecurity best practices is an important first step to ensuring that AI tools are deployed by regulated entities in a manner that protects the confidentiality, integrity, and availability of ePHI.

Implications of the Proposed Modifications

While President Trump's January 20, 2025, memorandum entitled "*Regulatory Freeze Pending Review*," directed postponing effective date for the final and proposed rules, the comment period for the proposed modifications to the Security Rule has not been extended. Since the comment period ended on March 7, 2025, the proposed modifications, issued by OCR under the Biden Administration, have been under review by the Trump administration, which will decide whether to publish a final rule or withdraw it. Even if a final rule is issued, it could differ significantly from the NPRM. Nonetheless, the NPRM offers valuable insights on best practices related to cybersecurity standards for protecting ePHI to help avoid cyber and ransomware attacks, cyber breaches and potential OCR HIPAA civil monetary penalties.

Notably, in addition to bipartisan support for stronger healthcare cybersecurity requirements due to the ongoing rise in cyberattacks and data breaches, ERISA employee benefit plans, including group health plans, should pay close attention to their cybersecurity standards, as they must also comply with the DOL's cybersecurity guidance. [5] In light of the proposed modifications to the Security Rule and the government's growing focus on improving cybersecurity, group health plans, plan sponsors and their business associates should take appropriate action to follow cybersecurity NPRM best practice guidance.

[1] The 2003 HIPAA Security Rule adopted standards for the security of ePHI to be implemented by covered entities. Following the enactment of the HITECH Act, in 2013, HHS made minor modifications to the Security Rule to implement the HITECH Act's provisions that extended direct liability to business associates for compliance with the Security Rule.

[2] In April 2021, the Department of Labor's (DOL) Employee Benefit Security Administration for the first time ever issued cybersecurity guidance. This guidance was updated in September 2024, to, among other things, clarify and confirm that it applies to all types of ERISA plans, including health and welfare plans and all employee benefit plans.

[3] For example, the proposed new definitions include "Deploy," "Implement," and "Multi-factor authentication." The definitions that the NPRM proposes to modify include "Administrative safeguards," "Physical safeguards," and "Technical safeguards."

[4] In light of the rising cybercrime, National Institute of Standards and Technology (NIST) described "cyber resiliency" as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf)

[5] On November 21, 2024, the new bill, *The Health Care Cybersecurity and Resiliency Act of 2024*, was introduced by HELP Committee ranking member Dr. Bill Cassidy, R-La., along with Sens. Mark Warner, D-Va., John Cornyn, R-Texas, and Maggie Hassan, D-N.H. This bill aims to strengthen healthcare organizations' ability to prevent and respond to cyberattacks and calls for improved collaboration between the HHS and the Homeland Security department's Cybersecurity and Infrastructure Security Agency (CISA) to address healthcare cybersecurity needs.

Direct-to-Consumer Prescription Drug Programs: Plan Sponsors Beware!

Mary E. Powell

We are pleased to share this recent article from the Daily Journal, written by our colleague Mary Powell. Mary focuses her employee benefits practice on health and welfare plans, and she advises plan sponsor and other fiduciaries of those plans regarding their duties and obligations under the Employee Retirement Income Security Act of 1974 (ERISA).

Recently, Mary has been writing and speaking extensively on the often misunderstood (and therefore overlooked) fiduciary obligations that must be met to properly monitor Pharmacy Benefit Managers (PBMs), the intermediaries who manage and administer prescription drug benefits for self-funded group health plans, for which they often receive substantial compensation. In this Daily Journal article, Mary addresses important contractual issues that can arise when health plan fiduciaries attempt to save costs by eliminating the PBM, through the implementation of direct-to-consumer (DTC) prescription drug programs. The legal issues for plan fiduciaries can be complex and often come as a surprise. That said, these issues are manageable and the applicable ERISA standards can be met, if properly understood and addressed.

Click here to read the article published in the Daily Journal. (https://www.truckerhuss.com/wp-content/uploads/2025/04/Direct-to-Consumer-Prescription-Drug-Program-Mary-Powell-Trucker-Huss-Daily-Journal.pdf)

PUBLICATION INFO:

The Trucker Huss Benefits Report is published monthly to provide our clients and friends with information on recent legal developments and other current issues in employee benefits. Back issues of the Benefits Report are posted on the Trucker Huss website (www.truckerhuss.com (https://www.truckerhuss.com))

Editor: Nicholas J. White, nwhite@truckerhuss.com (mailto:nwhite@truckerhuss.com)

In response to IRS rules of practice, we inform you that any federal tax information contained in this writing cannot be used for the purpose of avoiding tax-related penalties or promoting, marketing or recommending to another party any tax-related matters in this Benefits Report.

SAN FRANCSICO
135 Main Street, 9th Floor
San Francisco, California 94105-1815

LOS ANGELES
15760 Ventura Blvd, Suite 910
Los Angeles, California 91436-3019

PORTLAND
329 NE Couch St., Suite 200
Portland, Oregon 97232-1332

Tel: (415) 788-3111
Fax: (415) 421-2017
Email: info@truckerhuss.com (mailto:info@truckerhuss.com)
Website: www.truckerhuss.com (https://www.truckerhuss.com)