THE EXCELLENT FIDUCIARY

The Deep End of the Vendor Pool

*by Ronald E. Hagan**

Changes in regulatory rules and guidelines expand the categories of vendors who fall within an employer's duty to monitor service providers for their qualified employee benefits plans. Surprisingly, many employers that sponsor such programs are unprepared and unresponsive to those changes.

INTRODUCTION

Concerns exist that employers that sponsor employee benefits plans under the Employee Retirement Income Security Act of 1974 (ERISA) have not expanded their vendor monitoring activities to keep pace with current regulatory rules and guidelines. External forces such as rampant data breaches of retirement and health plans and excessive compensation arrangements with health plan providers have changed the makeup of a compliant vendor monitoring program. This article examines the impact of these developments and what human resources and finance leaders need to do to meet the sea change in plan administration they represent.

DATA SECURITY SURPASSES MOST OTHER PRIORITIES

A report by the General Accounting Office (GAO) recommending federal guidance to reduce cybersecurity risks in retirement plans had a dramatic effect in 2021. That report, combined with ever-increasing cyber threats to plan participant data and plan assets, drove the U.S. Department of Labor (DOL), through its enforcement arm, the Employee Benefits Security Administration (EBSA), to publish cybersecurity guidance for plan sponsors of ERISA qualified plans. The EBSA swelled the range of service provider categories embraced within ERISA's fiduciary rules to include vendors not traditionally tracked by employee benefits plan committees. Up to now, recordkeepers and mutual fund managers have been at the core of vendor monitoring exercises. The reason for that emphasis has roots in the evolution of retirement and pension plan investments as the dominant concern among employers. Illustrating that development is the many plan fiduciary management teams that retain the title "Investment Committee."

Our examination of scores of fiduciary committee meeting

**RONALD E. HAGAN* is chairman of RolandlCriss, the premier risk manager for retirement plan sponsors, foundations, and endowments. Mr. Hagan has a lengthy career in enterprise risk management. He has pioneered many of the certification, standards practices, and fiduciary risk management strategies preferred by boards of directors and human resources executives. Reach him by e-mail at ronhagan@rolandcriss.com.

agendas reveals that investment-related items continue to dominate the list of scheduled talking points. Despite solid evidence that fiduciary violations and data security risks are far more apt to occur in retirement plan administration and health and welfare (H&W) plan oversight, well removed from the investment discipline.

The absence of data security as a scheduled topic in most of those meeting agendas suggests the possibility that a widespread lack of attention to the EBSA's clarion call for action exists across the fiduciary community.

The information technology departments of most organizations maintain a data security policy at the enterprise level but rarely do such policies expand to include ERISA plans' personally identifiable information (PII) and protected health information (PHI). Bryan Smith, the section chief for the FBI's Cyber Division, warns that cybersecurity is more a business challenge than an IT issue. During a public event, he stated:

> The value of information is dependent on the degree to which it affects the viability of an enterprise. The more critical the data, the more emphasis is needed on securing it. An IT department is not the best-equipped office to prioritize the value of all corporate information.

That view shifts responsibility from IT departments to fiduciary committees for ERISA-qualified plans.

If the security and confidentiality of employee benefits plan data and assets are to gain better protection, fiduciary committees must alter their focus. That starts with broadening the array of vendors they monitor. Most committees will need to expand their oversight to cover all their employers' sponsored employee benefits plans and acquire new skills in order to evaluate service providers they likely have not previously considered in their monitoring efforts.

In addition to the impact of cybersecurity controls on H&W plans by the EBSA's rules, fiduciary responsibility for those programs enlarged even further recently. ERISA requires retirement plan sponsors to ensure the fees paid to vendors of services to their plans are reasonable. The U.S. Congress recently thrust a similar responsibility on employers for H&W plans requiring them to engage providers of services under only proper fee arrangements. The following paragraph discusses that development in more detail.

GROUP HEALTH AND WELFARE PLANS REQUIRE ELEVATED ATTENTION

The Consolidated Appropriations Act (CAA) is a provision that requires group health plan brokers and consultants to make comprehensive fee disclosures similar to those that apply to retirement plans. The CAA's fee disclosure requirements result in additional compliance obligations for group health plan sponsors. Simply put, the CAA requires that compensation paid to health plan providers is reasonable.

A change in ERISA § 408(b)(2) in 2012 required vendors to fully disclose the fees they charge retirement plans. That code section in ERISA is often referred to in retirement plan circles as the "Fee Rule." It mandates that plan fiduciaries examine their vendors' disclosures and validate the reasonableness of their compensation.

The Fee Rule has dramatically affected recordkeeping fees, investment consulting pricing, and plan fiduciary management practices. It also formed the basis for an explosion of lawsuits alleging breaches of fiduciary duty by employers and their benefit plan committee members that shows no signs of slowing. According to fiduciary insurance underwriter Chubb, settlements in excessive fee class action lawsuits between 2016 and 2020 were nearly $1 billion.[1]

The CAA's disclosure rule mirrors the Fee Rule and comes with a nearly identical responsibility for employers to document their opinions of the fairness of group health plan vendors' fees.

CONFORMING TO THE CAA

Four actions comprise best practices for employers that sponsor H&W plans:

- Expand the charter of the committee that oversees the enterprise's retirement plan to include the responsibility of managing H&W plan service providers and soliciting and evaluating the required disclosures. The disclosures must be received "reasonably in advance" when the service provider contract or arrangement is entered, extended, or renewed.
- Implement a written policy or procedure to identify the committee's duties, the required elements of disclosure (which differ depending on the type of service provider), and the process for responding to a service provider that fails to provide the required disclosures.
- Document the committee's review of the information disclosed and the report of its findings. Test an incumbent or proposed vendor's H&W plan fees against a reliable, independent third-party data aggregator or through a formal request for proposal (RFP). (Do not use vendors' or health consultants' benchmarking reports; they are unavoidably biased!)
- Consider hiring an independent expert to conduct the CAA fee assessment. Delegating the analytical work to an expert allows responsible plan fiduciaries to evaluate and compare the service provider's compensation with comparable service providers and industry standards. An expert in the Fee Rule can also help support the committee's decision-making process and document that a service provider's compensation is reasonable.

The twin events of the EBSA's announced cybersecurity best practices and the CAA's vendor compensation controls merit adding H&W plans to an employee benefits committee's charter.

THE CYBERSECURITY VENDOR POOL

Upon examining the EBSA's guidance, it is clear that the federal government is very concerned about the safety and confidentiality of workers' data. It emphasizes the duty of employee benefits plan fiduciaries to take steps to protect plan participants' PII and PHI. In order to execute that duty, steps must be "appropriate and necessary," and the "system" used to communicate with the participants must have embedded protections.[2]

In addition to retirement plan recordkeepers, other vendors process and store large amounts of PII and PHI on their computer systems. Consequently, it may surprise some employee benefits plan committees that the EBSA's cyber mandate will dramatically expand the scope of their supply chain management responsibilities.

The array of service providers with varying degrees of access to PII or PHI in defined contribution, defined benefit, and H&W plans takes their fiduciaries to the deep end of the vendor pool and includes at least 12 categories:

- Recordkeepers.
- Third-party administrators.
- Investment consultants.
- Health plan consultants & brokers.

- H&W plan providers.
- Payroll providers.
- Commercial banks.
- Custodians.
- Attorneys.
- CPA plan auditors.
- Printers.
- IT consultants.

In addition to those listed above, some vendors introduce other organizations into the supply chain by contracting for help servicing their retirement, pension, and health plan clients. These so-called "subservice" enterprises comprise a class of fourth-party vendors that fall within the government's cybersecurity parameters and hence, plan sponsors' duty to select and monitor prudently.

ASSESSING THE SUPPLY CHAIN

Cybersecurity risk assessments for employee benefits plans have become essential for any management team. But, as the threat landscape continues to evolve, ensuring PII, PHI, and plan assets are not vulnerable to a potential attack has become more complicated. An assessment framework developed by the National Institute of Standards and Technology (NIST) is an excellent starting point for testing the cybersecurity readiness of an employee benefits plan complex. However, the EBSA's cyber initiative alters the usefulness of the NIST framework. While a NIST-driven assessment would produce valuable results, it falls short of preparing fiduciaries for an EBSA audit.

The lack of standards from the DOL or the EBSA for constructing an assessment methodology makes it challenging for human resources leaders to know where to start. However, we are aided somewhat by what we have learned about the government's cybersecurity audits.

When the DOL issues guidance like its cybersecurity best practices, ERISA plan sponsors usually have a year or two to prepare before the inevitable audit activity starts. Not so in this case. Only days after the EBSA announced its guidance, Roland|Criss learned about several investigations that the DOL started regarding cybersecurity practices. Those investigations began with the typical request for documents. The standard list of requested documents and records is, of course, extensive. In addition, the EBSA is requesting a nonstandard list of documents specific to cybersecurity. The scope and depth of the EBSA's cybersecurity-related requests will seriously challenge the ability of many plan sponsors to answer unless they are well prepared in advance. Accordingly, a cybersecurity risk assessment, conducted annually, is now a vital best practice for fiduciary committees.

THE RISK ASSESSMENT

A cybersecurity risk assessment helps ERISA plan sponsors to expose and prioritize issues that could undermine PII and PHI security. The risk assessment process should examine the policies and procedures of the benefits plans vendors. Unfortunately, there is no simple "Vendor Checklist." Service providers' technology platforms and management approaches vary, requiring significant expertise in their business models that may not be present in-house. Furthermore, integrating an ERISA cyber assessment with the plan sponsor's information technology unit typically demands time and expertise not available in the business units on which fiduciary responsibility lands heaviest (such as human resources and finance). Incidentally, if your plan's current advisor is not professionally equipped to address ERISA cybersecurity comprehensively, add a specialist to your fiduciary advisory team.

An excellent option is Cyber-Protect^{RC} offered by

Roland|Criss. Its design and methodologies align with the best practices guidelines published by the EBSA, Version 1.1 of the NIST's Cybersecurity Framework, and data security strategies promoted by the Cybersecurity and Infrastructure Security Agency (CISA). You may obtain more information by e-mail at ronhagan@rolandcriss.com.

CONCLUSION

Employee benefit plans committees tend to elevate consideration of their 401(k) and 403(b) plan investments to so high a priority that they often overlook other vital matters. Adopting a cybersecurity policy at the plan level and testing it periodically for execution is the ideal way to ensure that internal support systems and vendors in non-investment-related categories get the attention demanded by the EBSA and the CAA. Plan fiduciaries should now focus on the latter without neglecting the former.

NOTES:

[1]See Chubb's report titled Excessive Litigation Over Excessive Plan Fees, https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/fiduciary-liability-educational-materials/documents/pdf/2021-09-15_Excessive_Litigation_over_Excessive_Fees.pdf, for more details.

[2]See ERISA Regulation § 2520.104b-1(c)(1)(i)).