THE EXCELLENT FIDUCIARY

Questions Fiduciaries Ask

*Ronald E. Hagan**

During the last few months, human resources managers asked us intriguing questions related to their fiduciary practices. This article presents a sampling of those questions and the responses that we offered for their consideration.

Developments in American society in 2020 have had a dramatic impact on human resources and risk managers. Chief among those developments is the novel coronavirus (COVID-19) pandemic. It imposed a staggering burden on many decision-makers tasked with maintaining enterprise operations despite reduced staffing. Mergers among vendors of retirement plan services have compounded the situation. Reduced service levels and the loss of the personal touch caused by consolidations of recordkeepers and investment firms leave many 401(k) and 403(b) plan fiduciaries reeling under the consequences.

Over the past few months, my inbox has received absorbing questions from human resources and finance executives about issues related to their role as retirement plan committee members. This article contains a sample of the topics introduced by their questions.

Q. **Should our retirement plan committee be involved in our plan's annual financial audit? If so, what do we need to know?**

A. If an employer sponsors a 401(k) or 403(b) retirement plan that has 120 eligible participants on the first day of the plan year, an audit from an independent certified public accountant (CPA) is required. The plan must be audited in subsequent years until the *eligible participant* number drops below 100. An eligible participant is an employee of the plan sponsor who meets both the statutory Internal Revenue Service (IRS) requirements and the plan's terms at the beginning of the year. Even if they decide not to participate in the plan, such employees are still considered eligible participants. Terminated employees who have balances in the plan on the first day of the plan year count as eligible participants.

Auditors' written opinions fall into one of four categories that include:

- **Unqualified opinion:** The "clean audit."
- **Qualified opinion:** (he auditor was unable to gather sufficient evidence.
- **Disclaimer of opinion:** The auditor refuses to pro-

**RONALD E. HAGAN* is Chairman of the Risk Standards Committee of RolandlCriss, which is 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.

vide any opinion related to the financial statements.

- **Adverse opinion:** The auditor discovered material misstatements that affect the user's decision-making.

Audit reports are complicated to develop because some information on which CPAs rely is not available. Furthermore, recordkeepers are a frequent source of inaccurate information. For example, vesting of participants' benefits can produce its share of "material weaknesses," typically due to over-reliance on the recordkeeper's calculations, which can be in error.

Some of the typical hotspots that auditors encounter include the following.

1. **Definition of Compensation:** A widespread deficiency we see in plan audits is the incorrect application of the term "compensation" for employee deferrals or employer matching calculations. It is essential to clearly understand the definition of compensation in all of its nuances.
2. **Delays in Remitting Participants' Deferrals:** Even with payroll providers that automatically remit employee contributions to a plan's custodian, late remittances are a frequent cause of audit deficiencies. Late remittances require the offending employer to reimburse the plan for lost earnings caused by late payments. Late payments are often the result of an employer's confusion over the DOL's rule[1] that governs deferral remittances.
3. **Cybersecurity Controls:** The risk of loss from a cyber attack is a high priority concern on the list of your auditor's plan of examination. A data security policy is a vital governance document for Employee Retirement Income Security Act of 1974 (ERISA) plans. The lack of a policy that explicitly addresses a retirement plan's Personally Identifiable Information (PII) is almost certain to result in a written audit deficiency.

Retirement plan committees should review their plan's most recent audit, making note of any deficiencies cited by the auditor. Using the results of the review, fiduciaries should prepare now for next year's audit.

1. Resolve any exceptions that exist in the most recent audit.
2. Confirm that your firm's payroll system reconciles accurately with deferrals and distributions.
3. Obtain help from a qualified expert if your cybersecurity policy needs upgrading to cover PII. (Roland|Criss provides such help.)

Q. **Our recordkeeper just completed a merger with another vendor. How should we react?**

A. Consolidation among service providers like recordkeepers continued over the past year. A merger typically introduces changes to the operations, personnel, and technology platform on which a fiduciary committee relies. The merger of a retirement plan's service provider with another vendor is, in effect, a vendor change. Thus, the plan's fiduciaries are required to evaluate the surviving vendor as if it were a new service provider to the plan. Hiring and properly supervising vendors of services to ERISA plans are fiduciary acts governed by the duty of prudence and loyalty. Establishing and implementing a process to ensure prudent selection and monitoring of service providers is a critical step toward reducing regulatory problems. The U.S. Department of Labor (DOL) acknowledges that dealing with vendors can be complicated and risky. Complex due to confusing jargon and interlocking vendors. Risky because plan fiduciaries are at a significant information disadvantage.

Vendors are specialists in the design of their products, services, and compensation arrangements. Executives that buy from these vendors do not have the vendors' degree of specialization. The result? Vendors have a critical information advantage over their clients. The solution? The DOL suggests prudent fiduciaries should thoroughly evaluate their plans' vendors upon a merger event. The typical mechanism for doing so is a Request for Proposal (RFP). Since vendors control the significant amount

of information that RFPs generate, it is advisable to engage the services of an independent risk management expert who will not be overmatched by vendors' responses to an RFP.

Q. **What cybersecurity risk poses the most significant challenge, and what can we do to combat it?**

An increase in attacks on retirement plan accounts is accelerating during the COVID-19 pandemic. Many of those attacks result in fraudulent distributions of assets from the plan participants' accounts. For example:

- A former employee sued the Estee Lauder cosmetics company and its recordkeeper. She discovered three distributions were made from her retirement account without her knowledge or consent. The amount totaled $101,000. In the suit, the former employee claimed the employer and the vendor breached their fiduciary duty by failing to secure and protect her account.
- A hacker took nearly $200,000 from a Massachusetts retirement account by using a fraudulent bank account. The thief also invaded the employee's e-mail account and intercepted the bank's notice of a change to her account. As a result, she was unaware of what was happening until it was too late.

These and other cases illustrate the increased risk that some retirement accounts can face if plan administrators are not at the top of their game regarding cybersecurity, or even if plan participants don't practice necessary personal security measures.

A recent court ruling could have a long-term impact on the reach of lawsuits involving fraudulent disbursements from retirement plans.

In May 2020, a district court ruled, in the case of *Leventhal v. MandMarblestone Group, LLC,*[2] that plan sponsors can be equally liable with a recordkeeper when hackers steal from retirement accounts. They can also be accountable for inadequate security if the affected participants work remotely or without adequate safeguards.

The court's ruling portends a threat of liability that is broad in scope and could impact everyone that touches a retirement plan without regard to their fiduciary status.

Plan fiduciaries should produce educational materials or host employee training sessions to educate participants on steps they can take to safeguard their retirement assets.

Regardless of the protection recordkeepers or employers put into place to prevent fraud and cyberattacks, individual participant behavior creates the most risk. Participant education efforts should:

- Explain the dangers of sharing passwords, never changing passwords, or using passwords that are too simple.
- Educate participants about the evolving security measures recordkeepers have available to help protect their accounts. These might include two-factor authentication (2FA), automatic account lock features, or voice recognition software.
- Recommend that participants periodically monitor their accounts (including the importance of receiving and reviewing account notifications) so that they can mitigate any damage in the event their account is compromised. Many participants set up their retirement plan accounts and forget about them, so they may not notice fraudulent transactions on their accounts for months.

Q. **What area of retirement plan administration causes the most frequent DOL and IRS audit problems for employers?**

Like the hollow wooden Trojan horse in Greek mythology that concealed an invading force, payroll can secretly undermine the compliance efforts of every organization that sponsors an ERISA-qualified retirement plan.

The point at which a retirement plan and a payroll system intersect is a breeding ground for the most common violations of fiduciary duty. And they can be the most unwieldy to fix.

Payroll errors of any kind cost an organization money, whether directly or

indirectly. Often, the cost is at least two-fold, because the mistake itself has a financial penalty independent of the time and money required to correct it.

The annual financial audit performed by a plan's CPA will not necessarily catch all payroll deficiencies. A CPA's audit is focused primarily on financial transactions, not operational processes. So, it is vital to self-test periodically a plan's payroll dependencies.

During our operations assessment engagements that span several years, we have noted the frequent occurrence of six payroll operations deficiencies that trigger fiduciary duty violations that require major corrective action:

- **Definition of Compensation**—The ERISA plan's definition of compensation was not used correctly for all participants' deferrals and allocations.
- **Matching Contributions**—Employer matching contributions were not made to all appropriate employees.
- **Elective Deferrals**—Eligible employees were not allowed to make an "elective deferral" election.
- **Participant Loans**—Participant loans did not conform to the requirements of the plan document and were, therefore, prohibited transactions.
- **Hardship Distributions**—A distribution is not considered necessary to satisfy an immediate and heavy financial need of an employee if the employee has other resources available to meet the need, including assets of the employee's spouse and minor children.
- **Timely Deposits of Deferrals**—DOL rules require employers to deposit deferrals to the trust as soon as the employer can do so. The so-called "safe harbor" deadline is a myth.

Q. **I have heard the term "prudent process" used to describe the way that fiduciaries are to manage their duty. What is a prudent process?**

While the DOL expects ERISA fiduciaries to follow a formal management program, many retirement plans do not have such a program. A prudent process can be likened to an Internal Controls Policy. In addition to increasing the confidence level of fiduciaries as they execute their role, such a policy is a great tool for making IRS or DOL audits go more smoothly.

An Internal Controls Policy can satisfy the DOL's prudent process requirement by spelling out the procedures the in-house fiduciaries will follow to keep the plan in compliance with the huge number of technical rules that must be followed. It is not designed only to prevent overpayments or penalties, but has a broader purpose of ensuring that the plan is run properly.

An Internal Controls Policy will embrace practices such as monitoring all of the IRS' tax contribution limits, applying the right definition of compensation to determine contributions (using the wrong definition is a common problem according to the IRS), making sure that payouts start as required when participants are age 70½, ensuring that vendors' fees are reasonable, and testing data security methods and systems. In addition, it will include filing requirements, such as the ERISA Annual Report (Form 5500), and participant disclosure requirements. It will also spell out who is responsible for each requirement. (Ask the author of this article about Roland|Criss' ERISA Internal Controls framework.)

E-mail your questions and comments to ronhagan@rolandcriss.com.

NOTES:

[1]29 C.F.R. § 2510.3-102.

[2]Leventhal v. MandMarblestone Group LLC, 2020 Employee Benefits Cas. (BNA) 197040, 2020 WL 2745740 (E.D. Pa. 2020).