What You Need to Know about Retirement Plan Fiduciary Obligations & Risk Management

SHRM 401(k) SOLUTIONS
BY RAYMOND JAMES

Table of Contents

I. Introduction

As a plan fiduciary, plan sponsors must operate their plans exclusively for the benefit of participants and beneficiaries. They can be held personally liable for failing to fulfill their fiduciary obligations to their plan participants and, potentially, face costly civil and criminal penalties. Plan sponsors can never shed themselves fully of fiduciary responsibility with respect to their plans, regardless of the type or number of service providers they may enlist. The question then becomes, is there a way for plan sponsors to manage the scope of their fiduciary liability? The answer is yes, through a carefully crafted plan governance process and co-fiduciary arrangements [ERISA §405(a)]. The goal of the module is to help plan sponsors to 1) understand their role as a plan fiduciary and 2) become educated consumers of ERISA fiduciary services is an important function in today's increasingly litigious environment.

II. Learning Objectives

- Know ERISA's fiduciary rules, responsibilities and liabilities
- Understand what constitutes a prohibited transaction with an interested party
- List the penalties that may apply for fiduciary failures and prohibited transactions
- Differentiate between ERISA 3(16), 3(21), 3(38) and 408(g) fiduciaries
- List strategies and best practices to help plans sponsors manage fiduciary liability
- Understand fiduciary government correction programs

III. Background

A. Who is a plan fiduciary?

Under rules in effect since 1975, generally, a fiduciary is any person or entity that meets any of the following stipulations:

- Is named in the plan document as a fiduciary (e.g., the business owner sponsoring the plan);
- Has discretionary authority over the management of a retirement plan or its assets (e.g., a discretionary trustee);
- Offers investment advice with respect to plan assets for a fee (e.g., an ERISA §3(21) investment advisor)

B. Obligations and Risks (breach)

1. The federal law titled, the Employee Retirement Income Security Act of 1974 or "ERISA," requires plan fiduciaries to act solely in the interest of plan participants and beneficiaries for the exclusive purpose of providing benefits to participants and their beneficiaries; while incurring only reasonable expenses to administer the plan.

   A fiduciary's responsibilities are guided by four primary principles:
   - the exclusive benefit rule, under which a fiduciary must operate the plan in a way that solely benefits participants and beneficiaries;

- the prudent expert rule, that says fiduciary actions will be held to a standard of an experienced professional;
- the plan document rule, which says the fiduciary must follow the plan unless the terms of the plan contradict the rules of ERISA; and finally,
- the diversification rule, where a fiduciary must offer a wide range of investment options to help participants meet their investment needs and diversify their investments accordingly.

2. What plan transaction are prohibited?

   Certain transactions between a fiduciary (who is a "party in interest") and the plan are not permitted (unless an exemption applies). ERISA Section 3(14) contains a comprehensive list of who and what entities are considered parties in interest to an employee benefit plan. The list includes

   - A fiduciary
   - A person providing services to the plan (e.g., a financial advisor)
   - An employer
   - An employee organization
   - A greater than 50% owner of the employer

   An unlawful exchange between a plan and a party in interest is a prohibited transaction (PT) involving the

   - Sale, exchange or lease of property
   - Lending of money or other extension of credit
   - Furnishing of goods, services or facilities
   - A transfer or use of plan assets

3. Consequences of Fiduciary Failures

   What happens when fiduciaries fail to live up to the standard of care expected of them? ERISA notes that in cases of a breach of duty, a fiduciary

   - Shall be personally liable to make good on losses to the plan,
   - Shall be personally liable to return any profits resulting from the breach
   - May be removed as a fiduciary and
   - May be subject to civil and criminal penalties and fines

   For example, the Department of Labor may assess a civil penalty of 20% of the amount payable pursuant to a court order or settlement agreement with the DOL for a breach of fiduciary duty (or knowing participation in a violation). A fiduciary that willfully violates any reporting or disclosure requirement can be subject to a criminal fine of $5,000, imprisonment for one year or both (and in the case of an entity other than an individual, the fine can be as much as $100,000). Additional penalties can apply for more serious and deliberate offenses. For example, accepting kickbacks or embezzling funds in connection with an ERISA plan is a federal crime, punishable by a $10,000 fine, five years in prison or both.

   EXAMPLE:
   Federal court orders Kansas City Area Business Owner to Pay $4.3 Million in Restitution, Serve Prison Term for Fraud and Theft from 401(k) Plan

The IRS may also assess a 15% PT penalty tax pursuant to IRC §4975. The IRS has the ability to impose a 15 percent penalty on individuals who participate in a prohibited transaction (IRC Section 4975). The penalty applies per year on the amount involved, until the prohibited transaction is corrected. The IRS penalty may increase to 100 percent of the amount involved if the prohibited transaction is not corrected [ERISA Sec. 502(i) and IRC Sec. 4975]. In addition, a mandatory 20% DOL penalty applies to the amount recovered by the plan when a prohibited transaction is corrected [ERISA Section 502(l)]. Some of the amount paid to the IRS for a prohibited transaction under IRC Section 4975 can be used to offset the DOL penalty under ERISA 502(l).

IV. Day-to-Day Plan Sponsor Fiduciary Obligations

A. Execute and maintain a written plan document

Both the DOL and IRS require every qualified retirement plan be established and maintained pursuant to a written instrument [ERISA Section 402(a)(1) and (b) and IRC Section 401(a)]. The DOL seeks to protect the rights of participants while the IRS will provide tax-favored status for a plan that is maintained with a written plan document.

The law (ERISA) mandates the presence of certain plan language in the document to protect the rights of plan participants and beneficiaries.

All qualified plans must have specific language, including provisions addressing

- Named fiduciaries for the plan,
- Funding procedures,
- Plan operations and administration,
- Amendments and the authority to make amendments,
- Distribution procedures,
- Assets held in trust,
- Participants' and beneficiaries' rights, and
- A process by which participants and beneficiaries may appeal denials of their plan benefit claims.

In order to receive these special tax benefits from the IRS, a qualified plan must be recorded in a written format. The written documents must conform to provisions in the Internal Revenue Code and Department of Labor regulations. The plan document language must be up to date and consistent with current laws and regulations.

B. Funding obligations

1. Accuracy and timing of employee salary deferral contributions and/or designated Roth contributions

For small plans (i.e., plans with fewer than 100 participants), sponsors must ensure employee salary deferrals are deposited to the plan trust within seven business days of being withheld from participants' pay. This is pursuant to a special DOL safe harbor rule for small plans.

For large plans (i.e., plans with 100 or more participants), sponsors must ensure employee salary deferrals are deposited to the plan trust as soon as administratively feasible, and not later than 15 business days after the end of the month deferred.

2. Accuracy and timing of employer contributions

   Sponsors must follow the terms of the plan document regarding the types of employer contributions they make to their plans, if any. In order for a business to receive a tax deduction for contributions it makes to the company's qualified retirement plan, employer contributions, such as matching or profit sharing, must be made by the business's tax-filing deadline, including extensions.

3. Allocation formulas for employer contributions: Match and/or profit sharing

   If a plan sponsor has included a matching contribution provision in the plan document, the employer can make matching contributions according to the allocation formula specified for eligible participants who contribute elective deferrals and/or designated Roth contributions. For example, a matching contribution allocation formula might be 50 cents for each dollar deferred by a participant. Employer matching contributions can be discretionary (contributed in some years and not in others, depending on the company's decision and the language of the plan document) or mandatory, as in Safe Harbor 401(k) plans.

   If a plan sponsor has included a profit sharing contribution provision in the plan document, the employer can make such contributions according to the allocation formula specified for eligible participants. A profit sharing contribution is not contingent upon whether a participant defers into the plan or not.

   Generally, contributions to a profit sharing plan may not discriminate in favor of highly compensated employees. The conventional method of satisfying this nondiscrimination requirement is to allocate contributions for each participant based on the same percentage of pay — as under a pro rata allocation formula. More complex, contribution allocation strategies are available that often allow owners and other select participants to receive a greater share of the overall contribution as compared to other participants. As a result, owners often can receive the maximum contribution amount permitted by law while rank-and-file employees receive lesser amounts, and still satisfy nondiscrimination requirements. Because of these contribution allocation strategies, business owners, who may be hesitant to make a profit sharing contribution because of the expense of contributing to all eligible employees, may be able to maximize their own contributions while trimming overall contribution costs. Business owners should be aware that plan documentation and administrative costs to support these more complicated allocation formulas may be higher than for more conventional formulas. Some common phrases used to describe these contribution maximizing allocation strategies include "Social Security integration," "permitted disparity," "cross-tested," "age-weighted," and "new comparability."

   Social Security integration and permitted disparity both refer to an allocation method that allows participants with compensation above a certain level (often times the Social Security Taxable Wage Base) to receive additional contributions within prescribed IRS limits. A cross-tested strategy allows business owners to receive substantially higher contributions than rank- and-file employees, as long as

the projected benefits at retirement are equivalent. Age-weighted and new comparability plans are types of cross-tested arrangements.

C. Investment selection and monitoring

1. Process

   Recall that the diversification rule under ERISA requires a plan fiduciary (e.g., the sponsor) to offer a wide range of investment options to help participants meet their investment needs and allow them to diversify their investments accordingly so as to minimize the potential for large losses. The plan sponsor has the fiduciary responsibility to prudently select and monitor the investment alternatives contained in the broad range of investment alternatives.

2. Documentation

   (ERISA) is clear that plans must "provide a procedure for establishing and carrying out a funding policy in a method consistent with the objectives of the plan" [ERISA §402(b)(1)]. Therefore, an employer who offers a retirement plan to his or her employees has a fiduciary responsibility under ERISA to put in place a prudent procedure for selecting, monitoring and replacing the investment options the plan offers to participants. To that end, a formal, written investment policy statement (IPS) can serve as documentation for this required investment procedure.

   For more details on an IPS, please see the section on Investment Policy Statement under Risk Mitigation Strategies.

D. Service provider selection and monitoring

Plan fiduciaries have a duty to prudently select and continue to monitor plan service providers. At the highest level, fiduciaries are expected to create a framework to monitor and assess the fees and services paid for and received by the plan to ensure the cost of services remains reasonable. This process should be well documented and reviewed periodically to assess the adequacy of the investments and services as they relate to the participants and beneficiaries. Lack of processes and benchmarks can indicate fiduciaries are not adequately discharging their fiduciary duties.

EXAMPLE: Court case *Tussey et al. v ABB, Inc., et al*

1. RFI/RFP

   A request for information (RFI) is a document used to gather information from potential plan service providers in order to create a shortlist of potential venders that will support a retirement plan. The purpose of an RFI is to collect information and compare businesses that are offering products or services that a needed to establish and properly maintain the plan. Plan sponsors typically collect this type of data for comparison as an initial step, to be followed by a request for proposal (RFP) to gather bids and move toward a formal contract with selected service providers. RFIs and RFPs are important forms of written evidence that supports the presence of a prudent fiduciary process.

While the DOL may not formally require plan sponsors to regularly request RFPs from plan service providers, the agency does assume " … plans normally conduct RFPs from service providers at least once every three to five years … " in anticipation of changes to fee and service disclosures.[1] In fact, the DOL has stated, "… in hiring any plan service provider, a fiduciary may want to survey a number of potential providers, asking for the same information and providing the same requirements. By doing so, a fiduciary can document the process and make a meaningful comparison and selection."[2]

Business owners who sponsor ERISA-governed plans for their employees, such as 401(k) plans, have a fiduciary duty to administer and manage their plans prudently and in the best interest of the plans' participants and beneficiaries. By extension, plan sponsors must follow a prudent process to both select and monitor any service providers engaged to support their plans. Therefore, requesting RPFs at regularly scheduled intervals can be part of an effective fiduciary liability reduction strategy and established plan governance program.

Court cases have provided more support for including a regular RFP process in plan governance. For example, the appellate court in *George v Kraft Foods Global Inc.,* No. 10-1469*,* WL 1345463 (7th Cir. Apr. 11 2011) held that plan fiduciaries who did not conduct RFPs every three years were at risk for fiduciary litigation. The case was eventually settled in 2012 for $9.5 million.

2. Benchmark

An important supplement to the RFP process is annual benchmarking. The two go hand in hand to help protect plan sponsors. A benchmark report will show how a plan's fees compare to the average in the marketplace, while the RFP process engages the plan sponsor and provides a means to evaluate the quality of those services.

The DOL assumes plan sponsors solicit RFPs for service providers every three to five years as part of their fiduciary duty to monitor plan servicer providers. Annual benchmark reports supplement the RFPs. Both are integral parts of a plan sponsor's fiduciary liability reduction strategy.

3. Service agreements

Service agreements outline the various relationships a plan sponsor may establish between its company and the providers hired to help maintain the sponsor's retirement plan.

Key provisions to look for in a service agreement relate to the following:

- Scope of services, including clearly defined responsibilities;
- Fees and method of payment;
- Who is able to amend the agreement and how can it be amendment;
- Who can terminate the agreement and how;
- Liability insurance;
- Confidentiality;

[1] https://www.gpo.gov/fdsys/pkg/FR-2010-07-16/pdf/2010-16768.pdf

[2] https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/meeting-your-fiduciary-responsibilities.pdf

- Ownership of intellectual property;
- Choice of Law (which state's laws will govern any disputes)
- How disputes are resolved and any monetary limits

Plan sponsors must ensure any service agreements with providers are consistent with the terms of their retirement plan documents.

4. Evaluate 408(b)(2) service provider disclosures

   Plan service providers must give a fee disclosure to plan sponsors at least annually in order to disclose direct and indirect compensation they receive of $1,000 or more. Failure to do so could result in a prohibited transaction requiring correction (return of compensation) plus a 15% penalty on the amount involved per year until corrected; interest and late penalties may also apply. The "408(b)(2) disclosure" requires a covered service provider that reasonably expects to be a fiduciary to an ERISA plan to disclose to the responsible plan fiduciary its status as a fiduciary, along with a description of its services and fees.

   Final Regulations Relating to Service Provider Disclosures Under Section 408(b)(2)
   https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/fact-sheets/final-regulation-service-provider-disclosures-under-408b2.pdf

E. Participant notices and disclosures

Tables from the DOL's guide
https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/reporting-and-disclosure-guide-for-employee-benefit-plans.pdf

Tables from the IRS's guide
https://www.irs.gov/pub/irs-pdf/p5411.pdf

F. Government reporting

The plan sponsor, potentially with the assistance of a plan administrator, is responsible for submitting various reporting forms to the IRS and DOL, including the following key reports. The following list is not all inclusive. Please refer to the IRS's website for a complete list. https://www.irs.gov/pub/irs-pdf/p5411.pdf

Form	Purpose
IRS Form W-2, Wage and Tax Statement	Report employee wages, federal withholding, active participant status, elective deferrals
IRS Form 945, Annual Return of Withheld Federal Income Tax	Report and remit federal withholding related to retirement plan distributions as reported on Form 1099-R
IRS Form 1099-R, Distributions from Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc.	Report retirement plan distributions
IRS Form 5330, Return of Excise Taxes Related to Employee Benefit Plans	Report various penalty taxes assessed against the plan
Series of IRS Forms 5500 and Schedules	Report the financial details of the retirement plan to the IRS and DOL
Form 5558, Application for Extension of Time To File Certain Employee Plan Returns	Request an extension of time to file IRS Forms 5500 and Form 5330

G. Data maintenance and record retention

ERISA Sections 107 and 209 are the two primary sections of law that cover the record retention requirements for qualified retirement plans. Proper data retention will assist plan sponsors with meeting their fiduciary duties of ERISA. In short, ERISA requires plan sponsors to retain plan-level records and reports, such as Form 5500 filings, for a period of six years after the filing date, and to keep participant-level records for an indefinite period of time.

Records	Plan Level	Participant Benefit
Authority	ERISA Sec. 107	ERISA Sec. 209
How long to keep	Six years	Indefinitely
What to keep	• Form 5500 filings • Associated schedules • Financial reports • Audited financial statements • Vouchers • Worksheets • Receipts • Resolutions	• Date of hire, rehire or termination • Participant eligibility date • Participant compensation • Contribution election forms • Participant's designated beneficiary • Records of any distributions requested by the participant • Qualified Domestic Relations Order • Plan loan documentation
Standard to Meet	Supporting information and documentation that would permit a plan sponsor to verify, explain and clarify plan records to the DOL, and allow the DOL to check for accuracy and completeness	Records sufficient to permit a plan sponsor to determine the benefits due or which may become due to plan participants. Failure to maintain required records for any plan year may result in a civil penalty of $10 for each employee with respect to whom such failure occurs.

Plan sponsors can retain these records via electronic media if they satisfy the following requirements:

1) The electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form;

2) The electronic records are maintained in reasonable order and in a safe, accessible place and in such manner as they may be readily inspected or examined;

3) The electronic records are readily convertible into legible and readable paper copy as may be needed to satisfy reporting and disclosure requirements or any other obligation under Title 1 of ERISA;

4) The electronic recordkeeping system is not subject, in whole or in part, to any agreement or restriction that would directly or indirectly, compromise or limit a person's ability to comply with any reporting and disclosure requirement or any other obligation under Title 1 of ERISA; and

5) Adequate records management practices are established and implemented.

V. Fiduciary roles under ERISA

A plan sponsor may allocate certain fiduciary duties to other named fiduciaries or other persons, if the plan document allows for this. A co-fiduciary is liable for another fiduciary's breach when:

- The co-fiduciary had actual knowledge of the other fiduciary's breach;
- The co-fiduciary knowingly participated in the breach or undertook to conceal it; and
- Damages resulted

To recap so far, when a retirement plan is established, there must be at least one fiduciary named to oversee and control the plan's operation. Fiduciaries are named through identification in the plan document or as a result of their function with respect to the plan. The Fiduciary Matrix graphic illustrates the types of fiduciaries that interact with retirement plans, and they are often referred to according to the pertinent sections of ERISA. Let's review plan fiduciaries by the sections of ERISA: 3(16), 3(21), 3(38) and 408(g).

A. 3(16) Plan Administrator "I will help you administer the plan."

Business owners who sponsor retirement plans that cover common law employees are deemed to be plan fiduciaries pursuant to ERISA Sec. 3(16). An ERISA Sec. 3(16) fiduciary acts as the plan administrator and is responsible for managing the day-to-day operation of the plan. The plan sponsor, generally, is the plan administrator unless he or she appoints another entity to assume some of the plan administrative functions. A plan sponsor can delegate certain ERISA 3(16) administrative responsibilities, for example

- Required compliance testing ;
- Plan eligibility notifications;
- Approval of participant loans and distributions; and
- Delivery of required participant notifications and disclosures.

Keep in mind that plan sponsors remain fiduciaries with respect to their plans, and can never fully disgorge themselves of fiduciary liability.

B. 3(21) Full-Scope Fiduciary "I will help you manage the plan and share the responsibility with you."

The broad definition of ERISA §3(21) applies to all plan fiduciaries, including the plan sponsor and trustee, for example. Generally, it includes anyone who has discretionary control over the plan and/or its assets in some respect.

C. 3(21) Limited-Scope Fiduciary "I will help you invest plan assets."

Under a written agreement that specifically outlines and limits his or her responsibilities with respect to the plan's investments, a 3(21) limited-scope investment advisor provides investment advice in a fiduciary capacity in exchange for a fee or other compensation.

Presently, the DOL applies a five-part test to determine whether a financial advisor is a fiduciary of a plan. The five-part test relates to making recommendations about the value of, or advisability of, investing in securities or other property. Under ERISA's 5-part test, a financial advisor is a fiduciary if investment recommendations

- Are made on a regular basis
- Are made pursuant to a mutual understanding
- Will form the primary basis for the recipient's investment decisions
- Are individualized to the plan
- Are given in exchange for a fee or other compensation

It is important to note that a financial advisor must satisfy all five criteria before he or she would be considered a fiduciary of a plan.

Investment advisors are fiduciaries who must make investment recommendations to other plan fiduciaries (e.g., the plan sponsor regarding the investment line up) that are in the best interest of their clients. However, investment advisors do not have the discretion to actually make the final decision regarding the investment line-up for the plan. That is left to the plan sponsor. Consequently, the limited-scope investment advisor is liable for his or her investment recommendations, but the plan sponsor retains fiduciary responsibility and liability for the final list of investment alternatives designated under the plan.

D. 3(38) "I will invest plan assets for you."

Historically, ERISA §3(38) was created to define the roles of multiple fund managers within a defined benefit plan. In contrast to a 3(21) investment advisor, a 3(38) investment manager has full investment discretion for the assets of a plan, generally, allowing the manager to make immediate investment decisions without the need for outside consultation or advance notice as, typically, would be the case with defined contribution plans.

Under ERISA, a plan sponsor is authorized to appoint an investment manager who will have responsibility for all investment matters, including the power to select appropriate investments, and acquire and dispose of plan assets [ERISA Section 3(38)(a) and 402(c)(3)]. The plan sponsor and all other plan fiduciaries are relieved

of all fiduciary responsibility for the investment decisions made by the investment manager [ERISA Section 405(d)(1)], provided certain conditions are met.

If the plan sponsor properly appoints an ERISA 3(38) investment manager and continues to monitored such individual or entity, then the plan trustee, the party that typically has direct responsibility for managing plan assets, will not be liable for the acts or omissions of the investment manager and will not be required to invest or otherwise manage any asset of the plan which is subject to the authority of the investment manager [ERISA §405(d)(1)].

Of critical importance, the plan sponsor does have a continuing responsibility to monitor whether the investment manager is actually performing the services.

There are several requirements with respect to the engagement of an ERISA 3(38) investment manager that a plan's named fiduciary (generally, the plan sponsor) must satisfy in order to avail itself of the fiduciary liability protection that an ERISA 3(38) investment manager can provide.

In order for an individual or entity to be considered an ERISA 3(38) investment manager, the person or entity must

- Be formally appointed and monitored by a named fiduciary of the plan;
- Have the power to manage, acquire or dispose of any asset of the plan;
- Be a registered investment adviser (RIA) under federal or state law, a bank as defined under the Investment Advisers Act of 1940, or an insurance company that is qualified to perform investment services under the laws of more than one state; and
- Acknowledge, in writing, that it is a fiduciary with respect to the plan.

If a plan uses the services of a person that does not satisfy all of the above criteria then the appointing fiduciary is not relieved of fiduciary responsibility, and will remain liable for the acts or omissions of the investment manager [see WHITFIELD v. *COHEN*, 9 EBC 1739 (S.D.N.Y. 1988)]. The case of *WHITFIELD v. COHEN* established the elements necessary for the prudent selection of a person or entity to invest ERISA plan assets. These considerations require the plan sponsor to

- Evaluate the person's qualifications including experience, education, registrations and past performance;
- Ascertain the reasonableness of fees;
- Review documents reflecting the relationship to be entered into; and
- Ensure adequate, periodic accountings in the future.

Following the proper procedure in selecting and monitoring an ERISA §3(38) investment manager is vital to ensuring the named plan fiduciary, usually the plan sponsor, will not be liable for the acts or omissions of the investment manager.

E. 408(g) "I will help plan participants invest."

An ERISA 408(g) fiduciary is someone that is called a "fiduciary adviser." The Pension Protection Act of 2006 (PPA-06) created a statutory prohibited transaction exemption for fiduciary advisers who deliver investment advice as part of an "eligible investment advice arrangement." A fiduciary adviser could be a registered investment adviser, a broker-dealer, an insurance company or a trust department of a bank, and this person

or entity is authorized by the plan sponsor to provide investment advice to participants through an eligible investment advice arrangement that is either based on a level-fee arrangement for the advisor, or a computer model or both. Fiduciary Advisers may also provide advice to IRA owners.

The investment advice program must meet several other requirements, including an independent audit, participant notices and disclosures, and record retention in order to qualify for the prohibited transaction exemption.

VI. Corrective options in the case of breach

A. DOL programs

Despite all our best efforts, plans sometimes face fiduciary violations. The Employee Benefits Security Administration (EBSA) division of the DOL is responsible for ensuring the integrity of the private employee benefit plan system in the U.S. EBSA's oversight authority extends to nearly 722,000 retirement plans. These plans cover about 154 million workers and their dependents and include trillions of dollars of assets.[3]

DOL Top Compliance Concerns

- Late deposit of deferrals
- Excessive service provider fees
- Imprudent investments
- Plan sponsor bankruptcies
- Abandoned pension plans
- Hard to value assets
- Fiduciaries that didn't know and/or fulfill their duties

In our next section we will address two DOL-sponsored fiduciary correction programs, namely the Voluntary Fiduciary Correction (VFC) Program and the Delinquent Filer Voluntary Compliance (DFVC) Program.

1. The VFC Program covers only certain fiduciary violations, including the

    - Delinquent participant contributions and participant loan repayments
    - Impermissible plan loans
    - Purchase of an asset from a party in interest
    - Sale of an asset by a plan to a party in interest
    - Sale and leaseback of real property to an employer
    - Purchase or sale of an asset by a plan from a person who not a party in interest at a price other than fair market value
    - Holding of an illiquid asset
    - Benefit payments based on improper valuation of plan assets
    - Duplicative, excessive, or unnecessary compensation paid by a plan
    - Improper payment of expenses by the plan
    - Payment of dual compensation to a plan fiduciary

[3] 2022 EBSA Budget Justification

The VFC Program consists of a four-step process.

Step 1: Identify any violations and determine whether they fall within the transactions covered by the VFC program

Step 2: Follow the process for correcting specific violations as outlined in the procedures provided by the Department of Labor

Step 3: Calculate and restore any losses or profits with interest, if applicable, and distribute any supplemental benefits to participants.
Step 4: File an application with the appropriate Department of Labor regional office

DOL Fact Sheet: Voluntary Fiduciary Correction Program

Voluntary Fiduciary Correction Program

2. Delinquent Filer Voluntary Compliance (DFVC) Program

A second fiduciary correction program is the DOL's Delinquent Filer Voluntary Compliance Program (DFVCP). The DOL's Delinquent Filer Voluntary Compliance Program is an effort to encourage pension plan sponsors to file overdue annual plan reports (commonly referred to as the Form 5500). The DOL's provides business owners with the opportunity to pay a reduced civil penalty for voluntarily complying with the annual reporting requirements through the DFVC program. Business owners are able to take advantage of the Delinquent Filer Voluntary Compliance Program only if they do so prior to being notified in writing by the Department of Labor of a failure to file a timely annual report.

DOL Fact Sheet DFVCP

Delinquent Filer Voluntary Compliance Program

B. IRS correction programs

Despite their best efforts, plan sponsors may find their qualified retirement plans fail to comply with all of the IRS's requirements. To address these situations, the IRS created the Employee Plans Compliance Resolution System (EPCRS) as a way to permit plan sponsors to correct plan qualification failures that could jeopardize the qualified status of their plans and, thereby, allow them to continue to provide their employees with retirement benefits on a tax-favored basis. The components of EPCRS are the Self-Correction Program (SCP), the Voluntary Correction Program (VCP), and the Audit Closing Agreement Program (Audit CAP).

The IRS has updated the EPCRS in Revenue Procedure (Rev. Proc.) 2021-30, which modifies and supersedes Rev. Proc. 2019-19, the most recent prior consolidated statement of the correction programs under EPCRS. This update to Rev. Proc. 2019-19 is a limited update and is published primarily to:

(1) expand guidance on the recoupment of Overpayments;

(2) eliminate the anonymous submission procedure under VCP, effective January 1, 2022;

(3) add an anonymous, no-fee, VCP pre-submission conference procedure, effective January 1, 2022;

(4) extend the end of the SCP correction period for significant failures by one year (which has the result of also extending the safe harbor correction method for Employee Elective Deferral Failures lasting more than three months but not beyond the extended SCP correction period for significant failures);

(5) expand the ability of a Plan Sponsor to correct an Operational Failure under SCP by plan amendment; and (6) extend by three years the sunset of the safe harbor correction method available for certain Employee Elective Deferral Failures associated with missed elective deferrals for eligible employees who are subject to an automatic contribution feature in a § 401(k) plan or § 403(b) Plan (from December 31, 2020, to December 31, 2023).

1. SCP

   A plan sponsor may correct certain plan failures without contacting the IRS or paying any fee. SCP is only available for correcting operational failures, which involve a failure to follow the terms of the plan document, and certain plan document failures. A plan sponsor that has established compliance practices and procedures may, at any time without paying any fee or sanction, correct insignificant Operational Failures under a qualified plan or a 403(b) plan. For a SEP or SIMPLE IRA Plan, SCP is available only if the SEP or SIMPLE IRA Plan is established and maintained on a document approved by the IRS.

   The plan sponsor generally may correct even significant Operational Failures and certain Plan Document failures without payment of any fee or sanction if the correction is made within the "correction period," which is the last day of the third plan year for which the failure occurred. If outside the three-year period, then SCP is available only if the failure is considered an insignificant Operational Failure.

   Under Rev. Proc. 2021-30, plan sponsors may correct an operational failure via plan amendment that increases a benefit, right, or feature.

2. VCP

   VCP permits a plan sponsor to correct certain plan failures any time before audit by filing a submission, paying a fee and receiving an IRS approval for correction of plan failures (an IRS "Compliance Statement"). The plan sponsor must correct the identified mistakes within 150 days of the issuance of the Compliance Statement. While the IRS is processing the submission, the IRS will not audit the plan, except under unusual circumstances. There are special procedures for anonymous and group submissions. The fee to submit a plan failure is based on the most recently filed Form 5500.

   Top Plan Failures Corrected Under VCP https://www.irs.gov/retirement-plans/top-ten-failures-found-in-voluntary-correction-program

   1. Failure to timely amend the plan for tax law changes

   2. Failure to follow the plan's definition of compensation for determining contributions

   3. Failure to include eligible employees in the plan

4. Failure to exclude ineligible employees from the plan
5. Plan loans
6. Impermissible in-service withdrawals
7. Failure to satisfy RMDs
8. Employer eligibility failure
9. Failure to timely correct ADP/ACP tests
10. Failure to provide top-heavy minimum contributions
11. Failure to satisfy the annual additions limit

3. Audit CAP

   If a failure (other than a failure corrected through SCP or VCP) is identified on audit, the plan sponsor may correct the failure and pay a sanction. The sanction imposed will bear a reasonable relationship to the nature, extent, and severity of the failure, taking into account the extent to which correction occurred before audit. The sanction paid under Audit CAP will be not be less than the fee paid under VCP.

   Correcting Plan Errors https://www.irs.gov/retirement-plans/correcting-plan-errors

VII. Risk mitigation strategies

A. Documentation and a Prudent Plan Governance Process

One of the best means to mitigate fiduciary liability is for a plan sponsor to establish, document and follow a prudent plan governance process with respect to plan decisions and actions. The governance process should include the following steps.

- Identify and record all plan fiduciaries, their roles and the responsibilities of each;
- Assess plan documentation for compliance and consistency, including
  - ✓ Governing documents
  - ✓ Trust agreement
  - ✓ Summary plan description
  - ✓ Participant notices and disclosures
  - ✓ Investment policy statement
  - ✓ Fidelity bond
  - ✓ Any reporting forms (e.g., Form 5500)
  - ✓ Service provider agreements (e.g., recordkeeping, financial advisor, etc.)
- Select and monitor the plan's investment committee;
- Develop and follow an investment policy statement;
  - ✓ Select and monitor plan service providers;
  - ✓ Evaluate plan operations and administration procedures;

- ✓ Compile evidence that the fiduciary process and procedures were followed (e.g., committee notes, board resolutions, plan documentation); and
- ✓ Reassess the plan and the process on an ongoing basis.

Under ERISA, fiduciaries are required to operate their retirement plans in the best interests of their employees or be subject to fines and penalties. To that end, an annual fiduciary review or checkup can be an invaluable part of a preventative care program for a plan and its sponsor, and should be part of the plan's documented fiduciary procedures. Following the audit, plan fiduciaries should

- Assess any fiduciary gaps,
- Implement fiduciary liability reduction tactics,
- Document the process in writing and preserve the records permanently, and
- Reassess the plan on an ongoing basis (at least annually).

Fiduciary liability reduction tactics may include, but are not limited to, identifying co-fiduciaries and documenting their responsibilities; creating and following an investment policy statement; adhering to the provisions of ERISA Sec. 404(c) to relieve the plan sponsor of liability for participants' investment decisions; including a qualified default investment alternative in the plan's investment line up; satisfying plan fee disclosure and reporting requirements; and considering plan design alternatives to better meet participant retirement outcomes.

B. Fiduciary Liability Insurance and ERISA Fidelity Bond

Many plan sponsors are not aware of the difference between an ERISA fidelity bond and fiduciary liability insurance. They are not the same. ERISA fidelity bonds and fiduciary liability insurances offer two distinct types of protection for plan fiduciaries. An ERISA fidelity bond is required by law; fiduciary liability insurance is optional, but potentially a prudent safety net. An ERISA fidelity bond is required by law to cover plan losses as a result of fraud or dishonesty by persons who handle plan assets. In contrast, fiduciary liability insurance insures fiduciaries, and in some cases the plan, against losses caused by breaches of fiduciary responsibilities. Fiduciary liability insurance in not required, but may be a good idea to help protect plan fiduciaries financially.

The Department of Labor (DOL), under ERISA Sec. 412 and related regulations, generally requires that every fiduciary of an employee benefit plan and every person who handles funds or other property of a plan be bonded in order to protect the plans from risk of loss due to fraud or dishonesty on the part of the bonded individuals. The Department of Labor (DOL) has a handy hand-out entitled **Protect Your Employee Benefit Plan with An ERISA Fidelity Bond** that provides an overview of the bonding requirements and how to obtain a bond.

Through an examination of Forms 5500, the IRS has determined that one of the top two most common compliance issues among plans is not having adequate ERISA fidelity bonding. The amount of the ERISA fidelity bond must be at least 10% of the amount of funds the individual handles, subject to a minimum bond amount of $1,000 per plan. In most instances, the maximum bond amount that can be required under ERISA with respect to any one plan official is $500,000 per plan. However, the maximum required bond amount is $1,000,000 for plan officials of plans that hold employer securities. The DOL has the authority to file suit against plan fiduciaries for lack of, or failing to have, an adequate fidelity bond.[4] Please see the Department of Labor's Field Assistance Bulletin 2008-04 for more details on ERISA Fidelity Bonds. Fiduciary liability insurance, on the other hand, is insurance plan fiduciaries purchase to protect themselves

[4] See U.S. Labor Department sues officers of Dublin, Ohio, business to restore funds to 401(k) plan and Lack of Fidelity Bond Precipitates Labor Department Lawsuit

in the event they breach their fiduciary responsibilities with respect to the plan. Remember, courts can hold plan fiduciaries personally liable for losses incurred by a plan as a result of their fiduciary failures. Fiduciary liability

insurance—while not required—could be an important financial safety net for plan fiduciaries. During a DOL investigation, the investigator will inquire whether the plan fiduciaries have such insurance.

Evolving demands have led to important expansions in fiduciary liability insurance coverage. Once limited to protecting trustees from fiduciary breaches and administrative errors, now enhanced policies can cover such things as the cost of plan corrections made through voluntary compliance programs, settlor and nonfiduciary claims, defense costs associated with regulatory investigations and regulatory penalties, which may not be paid from plan assets.[5]

ERISA fidelity bonds and fiduciary liability insurances offer two distinct types of protection for plan fiduciaries. An ERISA fidelity bond is required by law; fiduciary liability insurance is optional, but potentially a prudent safety net.

C. ERISA 404(c)

An employer can retain the responsibility for investing the plan's assets, or allow participants to self-direct all or a portion of their plan assets. Self-direction of investments is one of the requirements that an employer must meet if it chooses to take advantage of ERISA Sec. 404(c) fiduciary protection.

ERISA 404(c) provides a mechanism to shift investment responsibility from the plan sponsor to participants, thereby reducing the employer's fiduciary liability for investment performance. The formal requirements of ERISA 404(c) are numerous, but can be summarized into the following basic requirements. An employer will not be held responsible for the outcome of participants' investment decisions if a plan, such as a profit sharing, 401(k) or money purchase pension plan, gives its participants

- the ability to exercise control over the assets in their individual accounts;
- the ability to invest plan assets in a broad range of investment alternatives; and
- sufficient information about investment options under the plan that enables them to make informed investment decisions.

First, plan participants and beneficiaries must have control of assets and the opportunity to make periodic investment changes. Participant control of assets means that the participant must have a reasonable opportunity to give investment instructions to an identified plan fiduciary who is obligated to comply with such instructions. Others may not improperly influence a participant's selection of investments. The DOL will determine whether a participant has independent control over his or her assets based on the facts and circumstances of the situation. However, at least, participants must have the ability to change their investment elections at least quarterly or more frequently in light of market volatility.

If a participant fails to give investment instructions, then, except with respect to assets in a qualified default investment alternative (covered later), the employer does not receive ERISA 404(c) protection.

Second, for ERISA 404(c) relief, participants must be allowed to invest in a broad range of investments. That means, participants must have the ability to do all of the following.

[5] Aronowitz, Daniel, *Trends in Fiduciary Liability Insurance: What new Coverage Does Your Employee Benefit Plan Need?* Benefits Magazine; v52 no6 pp 18-24 Jun 2015

- Materially affect the potential risk and return on their account balances;
- Choose from at least three (or an adequate larger number of) diverse investment alternatives; and
- Diversify so as to minimize the risk of large losses, although diversification does not ensure a profit or guarantee against loss.

Keep in mind the business owner retains the fiduciary responsibility for prudently selecting and monitoring the investment alternatives contained in the broad range of investments.

Finally, participants and beneficiaries must receive adequate investment information, which includes, but is not limited to, receiving the following items:

- Description of investments,
- Information about investment managers,
- An explanation of when and how to make investments elections or changes,
- A statement of fees and additional disclosures as required under participant fee disclosure regulations,
- Information about shareholder voting rights and
- Name, address and phone number of the plan fiduciary.

A plan will satisfy the information requirements of ERISA 404(c) if plan participants receive the following:

- An explanation that the plan is a 404(c) plan and, therefore, the fiduciaries may not have liability for losses resulting from the participants' investment choices; and
- The information required under the participant disclosure regulations required under ERISA 404(a).

Furthermore, if a plan offers stock of the sponsoring employer as an investment alternative, the plan sponsor must provide participants with a description of the procedures established to provide for the confidentiality of information regarding holding and voting those securities, including contact information for the responsible plan fiduciary.

D. Investment policy statement

A plan sponsor is not required by law to have a written investment policy statement (IPS) for its plan — per se. However, the Employee Retirement Income Security Act of 1974 (ERISA) is clear that plans must "provide a procedure for establishing and carrying out a funding policy in a method consistent with the objectives of the plan" [ERISA §402(b)(1)]. Further, the DOL's Interpretive Bulletin (IB) 2008-02, as well as its predecessor IB 94-2, states that, "the maintenance by an employee benefit plan of a statement of investment policy designed to further the purposes of the plan and its funding policy is consistent with the fiduciary obligations set forth in ERISA §404(a)(1)(A) and (B)." It continues, "For purposes of this document [IB 2008-02], the term 'statement of investment policy' means a written statement that provides the fiduciaries who are responsible for plan investments with guidelines or general instructions concerning various types or categories of investment management decisions, which may include proxy voting decisions." IB 2008-02 also states, "statements of investment policy… would be part of the 'documents and instruments governing the plan' within the meaning of ERISA §404(a)(1)(D)."

Court rulings also support the need for an IPS. For example, in *Liss v. Smith*, 991 F. Supp. 278, 1998 U.S. Dist. LEXIS 238 (S.D.N.Y. 1998), the court found that based on the circumstances, it is necessary for a plan to maintain a written investment policy statement.

Therefore, an employer who offers a retirement plan to his or her employees has a fiduciary responsibility under ERISA to put in place a prudent procedure for selecting, monitoring and replacing the investment options the plan offers to participants. To that end, a formal, written IPS can serve as documentation for this required investment procedure.

The IPS is typically one of the first documents requested in a DOL investigation for potential fiduciary misconduct. The lack of an IPS may indicate a lack of fiduciary oversight. Arguably, the only thing worse than not having an IPS is having one in place and not adhering to its guidelines and documenting such.

Because there is no formal requirement to have a tangible IPS, there is no prescribed format or template for creating the statement. Despite the lack of formal guidance, an effective IPS includes:

- Objective and purpose of the investment policy for the plan
- Roles and responsibilities of key plan players (e.g., fiduciaries, third-party administrators, investment advisors, investment committee, etc.)
- Factors the plan will take into account when selecting investments
- Frequency and methodology for rebalancing investment portfolios
- Procedures for controlling and accounting for investment expenses
- Procedures for monitoring the investment policy on a continual basis
- Description of how the plan will select service providers

Although ERISA does not contain a specific requirement that a plan have a written IPS, such a document can serve as a fiduciary-friendly framework for selecting, evaluating and replacing plan investment options.

E. Qualified Default Investment Alternatives (QDIA)

ERISA 404(c) protection is expanded to include “qualified default investment alternatives” (QDIA) if certain notice and disclosure requirements are satisfied (effective 2007). In general, a QDIA is a life-cycle or target-date fund; balanced fund; or managed account that meet certain Department of Labor requirements.

Prior to PPA-06, the rules for selecting and monitoring default investments were vague at best. Traditionally, many plans defaulted to a stable value or money market fund. Generally, participants were not informed of the defaults, nor were the default funds subject to ongoing plan sponsor review or scrutiny.

PPA-06 addressed many of the outstanding issues with respect to ERISA 404(c) coverage and the use of default investments within a plan. Section 624 of PPA-06 added a new Section 404(c)(5) to ERISA. In general, as long as certain disclosure and notice requirements are satisfied, the participant’s contributions may be placed in default investment options and the plan will retain ERISA 404(c) protection.

PPA-06 mandates various requirements regarding default investment options. These requirements include the following.

1. The dollars must be invested in "qualified default investment alternatives (defined below).
2. Participants must have opportunity to direct their investments into other options.
3. A notice must be provided at least 30 days before the date of plan eligibility, or at least 30 days before the initial investment in a QDIA, and then at least 30 days before each subsequent plan year. The notice must be in a form deemed to be understandable by the average participant, and must contain the following information, a description of
    - when the participant's assets may be invested in the defaults;
    - the default, including investment objectives, risk and return characteristics, and fees and expenses;
    - the participant's rights to direct assets out of the default without fees or penalties; and
    - where the participant can obtain investment information concerning other investment options within the plan.
4. All account statements, proxies, prospectuses, etc., received by the employer must be forwarded to the participant.
5. Participants must be able to transfer from the default without penalty.
6. Participants must be afforded opportunity to invest in a broad range of investment alternatives.
7. Fees and expenses may not exceed the limits on such amounts that plans can impose on participants who opt out of the plan or decide to direct their investments.

Under the DOL final regulations, four types of investments are permitted as QDIAs.

The first option is a "life-cycle" or "target-retirement-date" fund or model portfolio that applies generally accepted investment theories, is diversified so as to minimize the risk of large losses, and is designed to provide varying degrees of long-term appreciation and capital preservation through a mix of equity and fixed income exposures based on the participant's age, target retirement date or life expectancy. Such products and portfolios must change their asset allocations and associated risk levels over time with the objective of becoming more conservative with increasing age. Asset allocation decisions for such products and portfolios are not required to take into account risk tolerances, investments or other preferences of an individual participant. For plans that use target date funds, the DOL has issued proposed regulations that, when finalized, will require plans to give employees more information about their target date fund and the changes to the percentage of stocks and bonds held in the fund as investors approach the target date.

A second option is a "balanced" fund or model portfolio similar to the first option, except that it must be consistent with a target level of risk appropriate for participants of the plan as a whole. Asset allocation decisions for such products and portfolios are not required to take into account the age, risk tolerances, investments or other preferences of an individual participant.

A third option is a "managed account," where participants' dollars are allocated based on age, target retirement date or life expectancy among the existing fund options in the plan by an investment

management service that applies generally accepted investment theories, allocates the assets of a participant's individual

account to achieve varying degrees of long-term appreciation and capital preservation through a mix of equity and fixed income exposures. Such portfolios must be diversified so as to minimize the risk of large losses and change their asset allocations and associated risk levels for an individual account over time with the objective of becoming more conservative with increasing age. Asset allocation decisions are not required to take into account risk tolerances, investments or other preferences of an individual participant.

A fourth, albeit limited, option is a capital preservation product. However, a plan may only use a capital preservation product as a QDIA for the first 120 days of an employee's participation. At the end of the 120-day period, the plan fiduciary must redirect the participant's investment in the capital preservation product to another QDIA. The DOL included this type of product for two reasons:

1. Because it realized that some plan sponsors may find it desirable to reduce investment risks for all or part of their workforce following employees' initial enrollment in the plan; and

2. To allow employees in automatic enrollment plans a reasonable amount of time following the end of the applicable 90-day withdrawal period to transfer assets to another QDIA.

A transition rule applies to plans that adopted certain stable value products with a guar- anteed interest rate as their default investment. The final rules grandfather these arrangements by providing relief for contributions invested in the default stable value investment on or before December 24, 2007. The transition rule does not apply to future contributions to stable value products.

The Department of Labor released has, on its web site (irs.gov), a three-page document entitled "Target Date Retirement Funds—Tips for ERISA Plan Fiduciaries," designed to assist plan fiduciaries in selecting and monitoring TDFs and other investment options in 401(k) and similar participant-directed individual account plans. The document highlights eight key considerations for plan sponsors when considering TDFs for their plans. The eight key considerations include the following:

- Establish a process for comparing and selecting TDFs
- Establish a process for the periodic review of selected TDFs
- Understand the fund's investments
- Review the fund's fees and investment expenses
- Inquire about whether a custom or non-proprietary target date fund would be a better fit for your plan
- Develop effective employee communications
- Take advantage of available sources of information to evaluate the TDF and recommendations you received regarding the TDF selection
- Document the process

F. Cybersecurity

Cybersecurity has been a growing topic of importance in the retirement services industry for years. The Bartnett v Abbott Labs et al court case in 2020 (although later dismissed), along with other cases, have heightened the concern for fiduciary liability related to such breeches. From a historical perspective, there is an

understanding under DOL Regulation Section 2520.104b-1(c)(i)(B) and other pronouncements related to the electronic delivery of plan information that a plan sponsor must ensure the electronic system it uses keeps participants' personal information relating to their accounts and benefits confidential.

Most recently, the DOL on April 14, 2021, issued three cybersecurity directives for retirement plans: one for plan sponsors, one for plan recordkeepers and one for plan participants:

- Tips for Hiring a Service Provider: This piece helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.
- Cybersecurity Program Best Practices: This piece assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks by following these steps.

    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 service provider are subject to appropriate security reviews and independent security assessments.
    7. Conduct periodic cybersecurity awareness training.
    8. Implement and manage a secure system development life cycle (SDLC) program.
    9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
    10. Encrypt sensitive data, stored and in transit.
    11. Implement strong technical controls in accordance with best security practices.
    12. Appropriately respond to any past cybersecurity incidents.

- Online Security Tips: This piece offers plan participants and beneficiaries who check their accounts online basic rules to reduce the risk of fraud or loss.

This trifecta of DOL guidance comes on the heels of two recommendations to the DOL from a February 2021 Government Accountability Office (GAO) report to: 1) formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to 2) establish minimum expectations for addressing cybersecurity risks in defined contribution plans. But despite the release of these three directives, presently, there is no comprehensive federal regulatory regime covering cybersecurity for retirement plans.

- Other Sources of Guidance to Consider

The American Institute of CPAs (AICIPA) has developed and maintains a cybersecurity risk management program, including a Systems and Organizations Controls (SOC) protocol intended to help plan sponsors in creating a strong cybersecurity framework for use by plan auditors. This Q&A, "Cybersecurity and employee benefit plans: Questions and answers," provides an overview of the resources.

The ERISA Advisory Council issued a report in 2016 entitled, Cybersecurity Considerations for Benefit Plans. The ERISA Advisory Council suggested the DOL raise awareness about cybersecurity risks and provide

information for developing a cybersecurity strategy specifically focused on benefit plans. "The Report" put forth considerations

for the industry for navigating cybersecurity risks. The considerations relate to the following three key areas. Please refer to the report for more details.

1. Establish a strategy
    - Identify the data (e.g., how it is accessed, shared, stored, controlled, transmitted, secured and maintained).
    - Consider following existing security frameworks available through organizations such as the Nation Institute of Standards and Technology (NIST), Health Information Trust Alliance (HITRUST), the SAFETY Act, and industry-based initiatives.
    - Establish process considerations (e.g., protocols and policies covering testing, updating, reporting, training, data retention, third party risks, etc.).
    - Customize a strategy taking into account resources, integration, cost, cyber insurance, etc.
    - Strike the right balance based on size, complexity and overall risk exposure.
    - Consider applicable state and federal laws.
2. Contracts with service providers
    - Define security obligations.
    - Identify reporting and monitoring responsibilities.
    - Conduct periodic risk assessments.
    - Establish due diligence standards for vetting and tiering providers based on the sensitivity of data being shared.
    - Consider whether the service provider has a cyber security program, how data is encrypted, liability for breaches, etc.
3. Insurance
    - Understand overall insurance programs covering plans and service providers.
    - Evaluate whether cyber insurance has a role in a cyber risk management strategy.
    - Consider the need for first party coverage.

The Report concludes with an appendix entitled, Employee Benefit Plans: Considerations for Managing Cybersecurity Risks (A Resource for Plan Sponsors and Service Providers).

State laws are another consideration. Each state has different laws governing cybersecurity concerns that may come into play. Unfortunately, many retirement plans cover multiple states or retirees who have moved out of state.

As fiduciaries of their retirement plans, the DOL requires plan sponsors to ensure the electronic systems they authorize for use in the administration of their plans keeps participants' personal information relating to their accounts and benefits confidential. While currently no comprehensive cybersecurity protocol for retirement plan administration exists at the federal level—we do have a series of guidelines, suggestions and best practices.

VIII. Conclusion

The Employee Retirement Income Security act was nearly 50 years ago to oversee qualified plans. Since then, the industry has evolved and plan sponsors are increasingly being held accountable for breaches to fiduciary duties. Plan sponsors and other fiduciaries face personal liability for their breach of duties under current ERISA guidelines.

But the news is not all bad. There is personal liability with ERISA, but this legislation is not a performance or outcomes based rule…it is more about the process and that is a good thing. As long as you follow AND DOCUMENT that you followed a prudent process, you should be ok. To go one further, sponsors are encouraged to hire prudent experts to help develop and execute this process.

Source: Retirement Learning Center

T: 833.440.401K (833.440.4015)
1 Crosfield Ave. Suite 102, West Nyack, NY 10994
Raymond James Home Office: 880 Carillon Parkway, St. Petersburg, FL 33706