SUMMER 2016
www.bdo.com

GET TO KNOW BDO – EXECUTIVE AND HR SERVICES

EBP COMMENTATOR

THE NEWSLETTER OF THE BDO EMPLOYEE BENEFIT PLAN AUDIT PRACTICE

CYBERSECURITY CONCERNS FOR EMPLOYEE BENEFIT PLANS

In recent months, the Department of Labor (DOL) has raised concerns about cybersecurity and employee benefit plans. Employee benefit plans may be vulnerable to cyber-attacks and thus exposed to risks relating to privacy, security, and fraud. Plan administrators, or those charged with governance, have an ERISA fiduciary duty with respect to the management of the plan, which encompasses the duty to care for personally identifiable information (PII) and protected health information (PHI).

Most plan sponsors and service organizations now use electronic means to conduct financial transactions for the plan (such as the remittance of participant and/or sponsor contributions) and to interface with participants (for instance, permitting participants to electronically initiate a new loan or request a plan distribution). It is these electronic records, and the related investment transactions, that may be at risk to a cyber-attack. Potential at-risk PII data includes information such as social security number, date of birth, email address, etc. While PII might seem to be an unlikely target, it has significant value to cybercriminals since it is permanently associated with an individual (unlike a credit card account number, PII cannot be easily "cancelled") and therefore can be exploited over a longer period of time.

For plans that utilize service organizations for most (or all) of their electronic records and investment transactions, a common misconception may be that those plans have relatively little risk if the service organization's SOC 1 report on controls has no issues. It is important to note that a SOC 1 report addresses a plan's internal control over *financial reporting*, but does **not** address the broader entity (or plan)-related cybersecurity controls and risk.

WHERE TO START?

Plan management and those charged with governance of a plan should evaluate their plan's cybersecurity governance as part of the overall risk assessment and start the discussion in the Audit, Administrative or Benefit Committee meetings. Some initial questions to help start the conversation include the following:

- Who is in charge of cyber security for the plan sponsor?
- Has this individual or department considered the potential cyber risks for the employee benefit plan?
- What would be plan management's response if notified of a data breach by one of their service providers or an employee? In such a situation, what would be the sponsor's obligation to the plan and to the participants?
- Has plan management identified the key individuals/providers involved in processes for the plan (e.g., who does what, when and how)?
- Does the sponsor require mandatory training on cybersecurity for all employees?
- What are the current legal and regulatory concerns?
- What are the applicable state laws should there be a data breach?

▶ Read more

CONTACT:

BOB LAVENBERG
Assurance Partner
National Partner In Charge of Employee Benefit Plan Audit Quality
215-636-5576
rlavenberg@bdo.com

CONTRIBUTORS:

Darlene Bayardo
Chelsea Smith Brantley
Anthony Cerasi
Kimberly Flett
Bob Lavenberg
Shahryar Shaghaghi
Joanne Szupka

For previously issued *EBP Commentator* newsletters or special editions, please visit www.bdo.com/publications/assurance/ebp.aspx.

A potential next step would be to then start cybersecurity discussions with the plan's third-party service providers and to review current policies or procedures relating to data security, including passwords, social media, document retention, internet privacy, etc. Even seemingly mundane employee-related policies may need to be considered since, according to a 2016 Association of Corporate Counsel Foundation report, employee error is the number one reason cited for cause of breach.

WHAT ABOUT CYBERSECURITY INSURANCE?

Cybersecurity insurance is a growing market. Most organizations are familiar with their commercial insurance policies, which provide general liability coverage to protect the business from injury or property damage. **However, standard commercial insurance policies may not cover cyber risks.** Since the specific cyber risks vary based on industry, policies for cyber risk are more customized than other types of insurance policies and can be based on a variety of factors. Such factors include the type of data collected and stored by the entity, the entity's presence on the internet, how employees and others are able to access data systems along with any IT updates and disaster response plans. Coverage may also include liability for security or privacy breaches, costs associated with a privacy breach or business interruption.

In summary, cybersecurity is a growing concern for all entities, including employee benefit plans. This issue is expected to become more pressing with each new announcement of a system failure or data breach. Plan management and those charged with governance need to assess their plan's risks and develop a specific strategy to address those risks as unfortunately, there is no "one-size-fits-all" approach related to cybersecurity.

AICPA EMPLOYEE BENEFIT PLANS (EBP) CONFERENCE

The recent AICPA EBP Conference (held May 2016) covered a wide variety of topics related to employee benefit plans, including updates from the federal regulators, key upcoming accounting and auditing changes impacting EBPs, etc. Below are some of the topics discussed:

- Accounting Standards Update (ASU) 2015-07, *Fair Value Measurement (Topic 820): Disclosures for Investment in Certain Entities That Calculate Net Asset Value per Share (or its Equivalent)* - removes the requirement to categorize investments for which fair values are measured using NAV as a practical expedient in the fair value hierarchy. However, it is required to disclose the amount measured using NAV as a practical expedient so that financial statement users can reconcile the fair value of investments included in the fair value hierarchy to total investments measured at fair value on the statement of net assets available for benefits.
- ASU 2015-10, *Technical Corrections and Improvements* – a change to the definition of "readily determinable fair value" (RDFV) has the potential to change previously reported fair value hierarchy levels for many investments that previously used the NAV as a practical expedient in both retirement accounts in plan sponsor financials as well as investments reported in EBP financial statements. Based on the revised definition of RDFV, investments such as pooled separate accounts (PSAs) and common/collective trusts (CCTs) may no longer qualify to use NAV as the practical expedient.
- ASU 2015-12, *Plan Accounting: Defined Benefit Pension Plans (Topic 960), Defined Contribution Pension Plans (Topic 962), Health and Welfare Benefit Plans (Topic 965): (Part I) Fully Benefit-Responsive Investment Contracts, (Part II) Plan Investment Disclosures, (Part III) Measurement Date Practical Expedient (ASU)* – reduces the complexity in EBP plan accounting; refer to our Winter 2016 edition for more details on the plan financial reporting simplification.
- Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 18, *Related Parties* – establishes requirements regarding the auditor's evaluation of a company's identification of, accounting for, and disclosure of relationships and transactions between the plan and its related parties for plans that are subject to filing Form 11-K with the Securities and Exchange Commission (SEC).
- Cybersecurity – cyber risks to EBPs is a current focus for the Department of Labor (DOL), who discussed its concerns as to how both plan sponsors and service providers are addressing plans' cyber risks. See also the article in this edition.
- DOL's Employee Benefits Security Administration (EBSA) - it was announced at the conference that the first and long-time Chief Accountant of the EBSA, Ian Dingwall, will be retiring effective January 2017.

▶ Read more

FORM 5500 UPDATE

2015 COMPLIANCE QUESTIONS

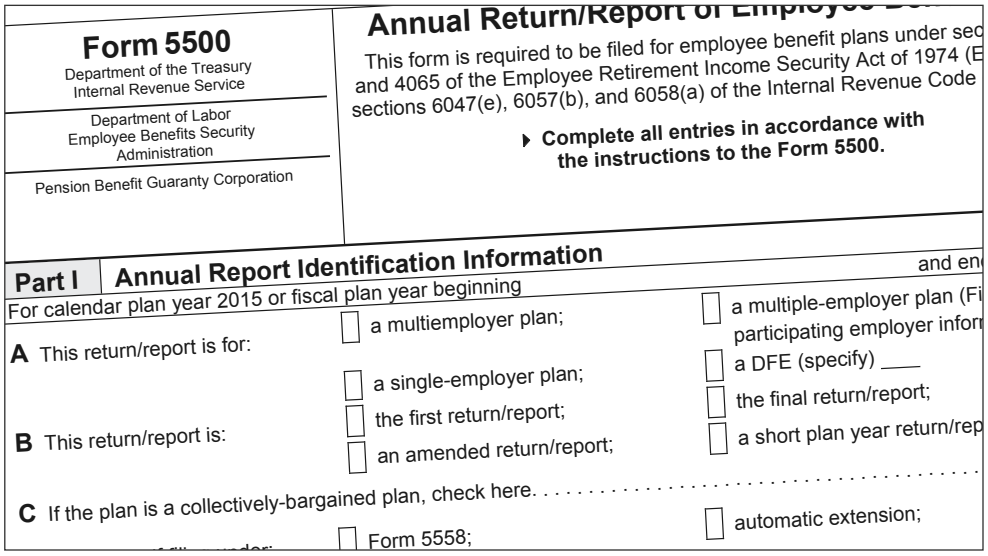
The Internal Revenue Service (IRS) instructed that plan sponsors should not answer the newly added compliance questions on the 2015 Form 5500 and Form 5500-SF (discussed in detail in our Winter 2016 edition) since the new questions had not yet been approved by the Office of Management and Budget (OMB).

2016 COMPLIANCE QUESTIONS

In March 2016, the IRS announced proposed changes to the 2016 Form 5500 Series returns (including Form 5500, Form 5500-SF and 5500-SUP). These changes incorporate updated/more consolidated versions of the 2015 compliance questions. Proposed questions include the following:

- The trustee, custodian and Form 5500 preparer's name and contact information
- Basic information regarding methods used by qualified plans to satisfy nondiscrimination requirements, including ADP/ACP testing methods and minimum coverage
- Timing of in-service distributions for plans subject to minimum funding including defined benefit and money purchase plans
- Whether a plan received a favorable advisory, opinion or determination letter with related information
- If required minimum distributions were made to more than 5% owners

The IRS also will provide a 2016 Form 5500-SUP that will be used to report these compliance questions to the IRS if these questions are not answered electronically on Form 5500 or Form 5500-SF. Form 5500-SUP will be a paper-only filing.



Form 5500
Department of the Treasury
Internal Revenue Service
Department of Labor
Employee Benefits Security
Administration
Pension Benefit Guaranty Corporation

Annual Return/Report of Employee
This form is required to be filed for employee benefit plans under sec
and 4065 of the Employee Retirement Income Security Act of 1974 (E
sections 6047(e), 6057(b), and 6058(a) of the Internal Revenue Code
▶ Complete all entries in accordance with the instructions to the Form 5500.

Part I Annual Report Identification Information
For calendar plan year 2015 or fiscal plan year beginning and en
A This return/report is for: ☐ a multiemployer plan; ☐ a multiple-employer plan (Fi participating employer infor
☐ a single-employer plan; ☐ a DFE (specify) ____
B This return/report is: ☐ the first return/report; ☐ the final return/report;
☐ an amended return/report; ☐ a short plan year return/rep
C If the plan is a collectively-bargained plan, check here.
☐ Form 5558; ☐ automatic extension;

FORM 5500 EXTENSION REMINDERS

Form 5558, *Application for Extension of Time to File Certain Employee Plan Returns*, is used to file for an extension of Form 5500, Form 5500-SF, Form 5500-EZ, Form 8955-SSA, and Form 5330. It permits an extension of two and a half months past the required due date (with a six-month extension for Form 5330).

A few reminders:

- For first-time filers of the Form 5500 series, Part II, Question 1 must be checked.
- Plan sponsors must use a separate Form 5558 for each return (it is not permissible to provide a listing of returns on one filing). However, a single Form 5558 may be used to extend both Form 5500 (or Form 5500-SF) and Form 8955-SSA for the same plan.
- A signature (generally the plan sponsor's) is required if extending the Form 5330, but not for extensions for the Form 5500 series or the Form 8955-SSA.
- Form 5558 is still a paper-only filing with the IRS (electronic filings are not available at this time).

▶ Read more

DOL "CONFLICT-OF-INTEREST" FIDUCIARY RULE RELEASED

In April 2016, the DOL released the final ruling regarding the definition of who is a fiduciary and its role with respect to providing investment advice. The new regulation (also referred to as the "conflict-of-interest" rule) is designed to close legal loopholes permitting retirement advisers to recommend investment products that are more profitable to the adviser and not necessarily in the best interests of their clients. This is the first significant regulation addressing investment advice since 1975 and reflects the greater role played by participants in investment decisions, through participant-directed 401(k) plans, individual retirement accounts (IRA), etc.

Prior regulations required an adviser to satisfy each part of a five-part test before the provider would be treated as a fiduciary adviser. If an adviser did not satisfy one of the tests, the adviser was permitted to operate with conflicts of interest that were not required to be disclosed to the client and was granted limited liability under the federal pension law. The conflict-of-interest rule replaces the five-part test and instead provides new broader set of principle-based rules along with exemptions to allow certain broker-dealers, insurance agents and others to act as fiduciaries while receiving compensation as long as they ensure that the advice provided is impartial and in the best interest of their clients.

Under the new regulation, a service provider is considered to be rendering investment advice if they receive fee-based or other compensation (whether directly or indirectly) that relates to providing guidance or assistance with the purchase or sale of securities or other investment property or the management of such investment property. The regulation stipulates what constitutes a "recommendation" and indicates that classification as a recommendation is based on the content, context, and presentation of the information and whether the information would be perceived as advising the recipient to partake in or refrain from taking a certain investment strategy.

A broad exemption under the regulation permits providers to receive compensation from selling certain products that might otherwise constitute a prohibited transaction. The Best Interests Contract (BIC) exemption is available if the provider offers only non-discretionary advice and meets certain other stipulations.

The final regulation also specifies that certain communications and activities are not considered to be recommendations, which addresses concerns noted during the proposal public comment period that recipients may come across information that should not be treated as fiduciary investment advice. Communications and activities excluded from the rule include the following:

- Participant education, such as certain interactive investment materials, which seek to provide participants/beneficiaries with investment options available under the plan
- General communications, such as newsletters or other broadly-focused communication not tailored to any one specific plan or participant.

Although compliance with the new regulations begins in April 2017, the DOL has adopted a phased implementation that includes a transition period from April 2017 to January 2018 for the various exemptions covered under the new regulations. This implementation period is expected to allow service providers to prepare for the compliance requirements and to adjust their status, if needed, from non-fiduciary to fiduciary status. For further details see webapps.dol.gov/FederalRegister/PdfDisplay.aspx?DocId=28806.

▶ Read more

THE PLAN SPONSOR'S FIDUCIARY ROLE

When discussing the role of the plan sponsor as the fiduciary to a plan, it is important to note that the role of fiduciary extends to specific individuals within the plan sponsor organization. Identifying those individuals depends on job functions performed on behalf of the plan and is not based solely on a particular job title. Within the plan sponsor organization, plan fiduciaries will often consist of a named plan fiduciary, any committees charged with the governance/ administration of the plan (which can include the audit committee, plan committee and/or a plan investment committee, etc.) as well an anyone else involved in decision making for the plan.

Once fiduciaries within the plan sponsor are identified, it is important that these individuals understand their role and responsibilities as set forth under the Employee Retirement Income Security Act of 1974 (ERISA). In brief, plan fiduciaries are to act solely in the interest of the plan participants with the overall goal of providing the participants with benefits. Fiduciaries are required to diversify the plan (per ERISA stipulations), ensure the plan is being administered in accordance with the plan document, monitor the plan's service providers, and ensure that the plan is only paying reasonable fees.

The plan sponsor's fiduciary duties and responsibilities encompass both the day-to-day plan administration and larger tasks such as timely filings with regulatory agencies and plan audits (if required). Since a fiduciary may not fully "delegate away" its responsibilities, the plan sponsor should ensure that third parties hired have the appropriate experience, qualifications and credentials, and performance record. Pod-casts of our four-part Fiduciary Gridiron series that discusses fiduciary considerations for plan sponsors may be accessed:

- **Part I –** www.bdo.com/events/fiduciary-gridiron-how-to-succeed-on-the-field
- **Part II –** www.bdo.com/events/fiduciary-gridiron-how-to-succeed-on-the-field-aug
- **Part III –** www.bdo.com/events/fiduciary-gridiron-how-to-succeed-on-the-field-nov
- **Part IV –** www.bdo.com/events/fiduciary-gridiron-how-to-succeed-on-the-field-jan

DID YOU KNOW?

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, individually identifiable health information for deceased individuals is protected for 50 years after the individual's death.

For more details, see www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

HELPFUL WEBSITES

http://www.dol.gov/ebsa/
http://www.efast.dol.gov
http://www.irs.gov/
http://ebpaqc.aicpa.org
http://asc.fasb.org

▶ Read more

CONSIDERING A DEFINED BENEFIT PLAN TERMINATION?

We invite plan sponsors who are considering possible termination of their defined benefit (DB) plans to listen to a podcast of a recent BDO webinar held jointly with Markley Actuarial Services Inc. and The Principal Financial Group. The *Guide Your Plan to Termination* podcast discusses current issues facing DB plans and potential options for sponsors and can be accessed at: www.bdo.com/events/defined-benefit-plan-webinar.

CRITICAL DATES FOR PLANS WITH DECEMBER 31ST (CALENDAR) YEAR ENDS

- **FIRST FORM 5500 DEADLINE - SUNDAY, JULY 31**
  (which automatically becomes Monday, August 1st)
- **FINAL FORM 5500 DEADLINE - SATURDAY, OCTOBER 15TH**
  (which automatically becomes Monday, October 17th). To be eligible for this extended deadline, Form 5558 must be filed on behalf of the plan on or before the first deadline.

BDO EBP PRACTICE

Nationally recognized in the field of employee benefit plan consulting and auditing, BDO audits nearly 1,900 plans ranging in size from 100 to close to 400,000 participants. Our engagements are staffed with accountants experienced with all types of audits including defined contribution (401(k), profit sharing, ESOP, and 403(b) plans), defined benefit (pension equity or cash balance) and health and welfare plans (defined benefit or defined contribution). We have extensive ERISA knowledge of audit and filing requirements, including full-scope, limited-scope, SEC Form 11-K filings and Master Trusts.

BDO's National Employee Benefit Plan Audit Group meets regularly to develop training and guidance and discuss updates in the industry and auditing practices. Our professionals are regular presenters at local, state and national seminars. We continue to be extensively involved with the American Institute of Certified Public Accountants (AICPA) National Conferences on Employee Benefit Plans. Many of our professionals serve in leadership roles in the accounting profession as senior advisors and are active members of several governing boards and CPA societies. For example, our professionals currently serve on various AICPA committees, such as the AICPA's Joint 403(b) Plan Audit Task Force (we are proud to have had representation at the chair level for this committee) and the AICPA Technical Standards Subcommittee of the Professional Ethics Executive Committee. BDO's EBP professionals have also served on the AICPA Employee Benefit Plan Audit Quality Center Executive Committee (immediate past chair) and the Employee Benefit Plan Expert Panel.

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through 63 offices and more than 450 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.