STRADLEY RONON

Fiduciary Governance

Risk&Reward
fiduciarygovernanceblog.com
@FidGovGroup

May 5, 2021

Springtime DOL Updates

As we await even more fiduciary-related rules and guidance from the U.S. Department of Labor (DOL) over the coming months, we take stock of some lower-profile spring updates worth noting. We begin with the DOL's recent cybersecurity guidance, the first of its kind, as cybersecurity becomes an increasingly important issue for plan sponsors and service providers. We conclude with some new DOL guidance related to locating missing plan participants.

Cybersecurity

On April 14, the DOL released a batch of guidance that attempts to clarify best practices for maintaining cybersecurity. The first of the guidance, aimed at plan sponsors and other fiduciaries, offers tips for hiring third-party service providers and ensuring they maintain strong cybersecurity practices. The second batch of guidance offers cybersecurity best practices for plan recordkeepers and plan fiduciaries. A final release offered tips for plan participants who access their account information online but will not be discussed here. These are the first cybersecurity guidance provided by the DOL.

The following tips offered by the DOL are designed to help fiduciaries meet their obligations under ERISA in prudently selecting and monitoring service providers:

1. Ask about the service provider's information security standards, practices, policies, and audit results and compare them to industry standards.

2. Ask the service provider how it validates its practices and what levels of security standards it has met and implemented. Consider looking at contract provisions that confer rights to review audit results demonstrating compliance with the standards.

3. Evaluate the track record of the service provider, including litigation brought against the service provider.

4. Ask if the service provider has experienced security breaches and, if so, what happened, how the provider responded, and how it was resolved.

5. Inquire if the service provider has insurance that would cover losses caused by cybersecurity and identity theft breaches.

6. Include ongoing compliance with cybersecurity and information security standards as a part of the service provider's contractual commitments. If possible, include terms that will enhance these protections, such as:

    a. Require the service provider to obtain an annual audit from a third-party to evaluate the service provider's compliance with information security policies and procedures.

    b. Clearly stated provisions outlining the service provider's obligations and restrictions on the use and sharing of information.

    c. Require notification of any cybersecurity breaches.

    d. Specific requirement to meet all federal, state and local laws, regulations, directives and requirements related to record retention, destruction, privacy, and security.

    e. Required insurance to cover losses related to cybersecurity losses. This may include professional liability, errors and omissions liability, cyber liability, and/or privacy breach insurance.

For more information, please contact:

George Michael Gerstein
Co-Chair, Fiduciary Governance
202.507.5157
ggerstein@stradley.com

John "JJ" Dikmak Jr.
Associate
215.564.8025
jdikmak@stradley.com

In the second batch of guidance, the DOL offered best practices for plan recordkeepers and other service providers responsible for plan-related data. The list also includes the best practices for a plan fiduciary hiring one of these service providers. These best practices include:

1. Have a formal, well-documented cybersecurity program. DOL highlighted 18 specific areas an effective policy would cover, including data governance and classification, access controls and identity management, business continuity and disaster recovery, configuration management, asset management, and risk assessment.

2. Conduct prudent annual risk assessments. The scope, methodology, and frequency of assessments should be codified.

3. Have a reliable annual third-party audit of security controls.

4. Clearly define and assign information security roles and responsibilities. This includes clearly defining the roles of upper management, especially the Chief Information Security Officer (CISO).

5. Have strong access control procedures which cover both authentication and authorization.

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. Perform cybersecurity awareness training at least annually.

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. This would include notifying law enforcement, informing insurers, investigations, providing plan participants with information to assist in preventing or reducing their loss, honoring contractual terms, such as notification requirements, and fixing the problems which caused the breach.

Missing Participants

Earlier this year, the DOL provided a set of best practices for fiduciaries of defined benefit and defined contribution plans to locate missing participants and beneficiaries. Some "red flags" that a plan's current approach may be insufficient for locating a missing or non-responsive participant include a large number of missing or non-responsive participants; missing, incomplete or inaccurate contact and other pertinent information (email, social security numbers, addresses, etc.), and the absence

of adequate policies and procedures for handling returned mail marked "return to sender," "wrong address" and the like.

The DOL's list of best practices (copied below) are those that "have proven effective at minimizing and mitigating the problem of missing or non-responsive participants." These practices are non-exhaustive, and some may be more appropriate for a particular plan than others. Ultimately, "[r]esponsible plan fiduciaries should consider what practices will yield the best results in a cost-effective manner for their plan's particular participant population."

1. Maintaining accurate census information for the plan's participant population

- Contacting participants, both current and retired, and beneficiaries on a periodic basis to confirm or update their contact information. Relevant contact information could include home and business addresses, telephone numbers (including cell phone numbers), social media contact information, and next of kin/emergency contact information. Well-run plans regularly reconfirm that the information in their possession is accurate.

- Including contact information change requests in plan communications along with a reminder to advise the plan of any changes in contact information.

- Flagging undeliverable mail/email and uncashed checks for follow-up.

- Maintaining and monitoring an online platform for the plan that participants can use to update contact information for themselves and their spouses/beneficiaries, if any, and incorporating such updates into the plan's census information.

- Providing prompts for participants and beneficiaries to confirm contact information upon login to online platforms.

- Regularly requesting updates to contact information for beneficiaries, if any.

- Regularly auditing census information and correcting data errors.

- In the case of a change in record keepers or a business merger or acquisition by the plan sponsor, addressing the transfer of appropriate plan information (including participant and beneficiary contact information) and relevant employment records (e.g., next of kin information and emergency contacts). [DOL] has found that in the context of an acquisition, merger, or divestiture, well-run plans make missing participant searches of plan, related plan (e.g., health plan) and employer records (e.g., payroll records) part of the collection and transfer of records.

2. Implementing effective communication strategies

- Using plain language and offering non-English language assistance when and where appropriate.

- Stating upfront and prominently what the communication is about – e.g., eligibility to start payment of pension benefits, a request for updated contact information, etc.

- Encouraging contact through plan/plan sponsor websites and toll-free numbers.

- Building steps into the employer and plan onboarding and enrollment processes for new employees, and exit processes for separating or retiring employees, to confirm or update contact information, confirm information needed to determine when benefits are due and to correctly calculate the amount of benefits owed, and advise employees of the importance of ensuring that the plan has accurate contact information at all times.

- Communicating information about how the plan can help eligible employees consolidate accounts from prior employer plans or rollover IRAs.

- Clearly marking envelopes and correspondence with the original plan or sponsor name for participants who separated before the plan or sponsor name changed, for example, during a corporate merger, and indicating that the communication relates to pension benefit rights.

3. Missing participant searches

- Checking related plan and employer records for participant, beneficiary and next of kin/emergency contact information. While the plan may not possess current contact information, it is possible that the employer's payroll records or the records maintained by another of the employer's plans, such as a group health plan, may have more up-to-date information. If there are privacy concerns, the person engaged in the search can request that the employer or other plan fiduciary forward a letter from the plan to the missing participant or beneficiary.

- Checking with designated plan beneficiaries (e.g., spouse, children) and the employee's emergency contacts (in the employer's records) for updated contact information; if there are privacy concerns, asking the designated beneficiary or emergency contact to forward a letter to the missing participant or beneficiary.

- Using free online search engines, public record databases (such as those for licenses, mortgages and real estate taxes), obituaries, and social media to locate individuals.

- Using a commercial locator service, a credit-reporting agency, or a proprietary internet search tool to locate individuals.

- Attempting contact via United States Postal Service (USPS) certified mail, or private delivery service with similar tracking features if less expensive than USPS certified mail, to the last known mailing address.

- Attempting contact via other available means such as email addresses, telephone and text numbers, and social media.

- If participants are non-responsive over a period of time, using death searches (e.g., Social Security Death Index) as a check and, to the extent such search confirms a participant's death, redirecting communications to beneficiaries.

- Reaching out to the colleagues of missing participants by, for example, contacting employees

who worked in the same office (e.g., a small employer with one or two locations) or by publishing a list of "missing" participants on the company's intranet, in email notices to existing employees, or in communications with other retirees who are already receiving benefits. Similarly, for unionized employees, some have reached out to the union's local offices and through union member communications to find missing retirees.

- Registering missing participants on public and private pension registries with privacy and cybersecurity protections (e.g., National Registry of Unclaimed Retirement Benefits), and publicizing the registry through emails, newsletters, and other communications to existing employees, union members, and retirees.

- Searching regularly using some or all of the above steps.

4. Documenting procedures and actions

- Reducing the plan's policies and procedures to writing to ensure they are clear and result in consistent practices.

- Documenting key decisions and the steps and actions taken to implement the policies.

- For plans that use third party record keepers to maintain plan records and handle participant communications, ensuring the record keeper is performing agreed-upon services, and working with the record keeper to identify and correct shortcomings in the plan's recordkeeping and communication practices, including establishing procedures for obtaining relevant information held by the employer.