TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

Employers and other sponsors of health, welfare, 401(k) and other types of pension plans often rely on service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help employers and other plan sponsors and plan fiduciaries meet their responsibilities under ERISA to prudently select and monitor such service providers, we prepared the following tips for plan sponsors of all types and sizes of ERISA plans:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial/health institutions.

    - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.

2. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.

3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.

4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).

6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants, such as:

    - **Information Security Reporting**. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

- **Clear Provisions on the Use and Sharing of Information and Confidentiality**. The contract should spell out the service provider's obligation to keep private information private, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.

- **Notification of Cybersecurity Breaches**. The contract should identify how quickly you would be notified of any cyber incident or data breach. In addition, the contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.

- **Compliance with Records Retention and Destruction, Privacy and Information Security Laws**. The contract should specify the service provider's obligations to meet all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information.

- **Insurance**. You may want to require insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage. Be sure to understand the terms and limits of any coverage before relying upon it as protection from loss, including ensuring that the policy covers cybersecurity breaches and incidents involving the plan.