EMPLOYEE BENEFITS LAW
INFORMATION MEMO
JUNE 21, 2021

DOL Issues New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers and Plan Participants

On April 14. 2021, the U.S. Department of Labor (DOL) issued much needed guidance concerning best practices for plan sponsors, fiduciaries, record-keepers, participants and beneficiaries pertaining to cybersecurity for retirements plans. The DOL's guidance focuses on three specific topics: hiring service providers; managing cybersecurity risks; and online security tips for participants to avoid risk of fraud and loss. Although the guidance was couched as "best practices," it is reasonable to interpret it as creating minimum cybersecurity standards and practices for retirement plans. The guidance specifies the duty of plan fiduciaries to protect plan data against cybersecurity breaches and attacks, and potentially signifies a precursor for the DOL to assess liability for damages stemming from plan data breaches in the future. Although the guidance did not address health and welfare plans, those plans may also wish to consider implementing these measures.

Here is a summation of some of the key points raised in the guidance, as well as some helpful insights to be considered in connection with the DOL's recommendations.

I. Hiring Service Providers

Under ERISA, plan fiduciaries must act prudently when selecting and retaining plan service providers. Since plan service providers are often relied upon to preserve and secure plan records and participant data, it is essential that fiduciaries ensure that service providers implement strong measures to defend this information against potential cyber threats. When retaining service providers, the DOL recommends that plan sponsors make certain that vendors have sufficient security systems in place to guard against attacks and prevent potential breaches. The DOL offered the following suggested practices when contracting with service providers:

- *Security Standards:* Review providers' security standards, practices and policies. Request audit results verifying the sufficiency of their security systems, and compare these results to industry standards. Plan fiduciaries should look for vendors who follow a recognized information security standard that validates its compliance and utilize an independent auditor to verify information security, system/data availability, processing integrity and data confidentiality.
- *Effectiveness Review:* Verify the security standards employed by service providers and their validation process to ensure their security practices comply with these requirements, and ensure that their audit results reflecting compliance are available for review.
- *Reputation in the Industry:* Check service providers' track record in the industry, including any public information related to prior security incidents, as well as any litigation and legal proceedings related to their services.
- *Prior Incidents:* Consider vendors' previous security breaches, reviewing all details regarding those incidents and their response to the attacks.

- *Insurance Coverage:* Review the service providers' cybersecurity insurance policies and their scope of coverage to address losses incurred from security breaches or identity thefts. Confirm whether their insurance coverage will cover breaches caused by both their own workforce, as well as external attacks. Consider requiring vendors to maintain additional insurance coverage (i.e., professional liability, errors and omissions liability, cyber liability and privacy breach insurance, and/or fidelity bond or blanket crime coverage). Confirm policy limitations before counting on such coverage for loss protection.
- *Ongoing Compliance:* Ensure that contracts require vendors to maintain their cybersecurity and information security standards originally agreed to by the parties throughout the term of the contract, and beyond (if applicable). Consider requiring notice in the event of a change in their systems which impacts their ability to meet this criteria, or deviations from their prescribed security standards.
- *Limitation of Liability:* Address any contractual provisions which seek to limit responsibility or liability of the service provider for cybersecurity breaches.
- *Reporting:* Require annual third-party audits to determine compliance with cybersecurity policies and procedures, and require access to the results of those reviews.
- *Data Usage:* Specifically dictate vendors' obligations to preserve the privacy of all confidential data, prevent any use or disclosure of confidential information without written permission, and incorporate a stringent standard of care to guard against the unauthorized use (or misuse), access, loss, disclosure, or modification of confidential information.
- *Records Retention and Destruction:* Specify vendors' obligations to comply with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of confidential information.
- *Notice:* Include terms requiring vendors to provide notice for any incident or breach, specifying the timeframe for such notice and mandating service providers' cooperation to investigate and address the cause of the breach.

II. Cybersecurity Best Practices

The DOL has provided a list of best practices for plan record keepers and other service providers to follow:

- Have a formal, well documented cybersecurity program;
- Conduct prudent annual risk assessments;
- Have a reliable annual third-party audit of security controls;
- Clearly define and assign information security roles and responsibilities;
- Have strong access control procedures;
- 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;
- Conduct periodic cybersecurity awareness training;
- Implement and manage a secure system development life cycle program;
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response;

- Encrypt sensitive data, both stored and in transit;
- Implement strong technical controls in accordance with best security practices; and
- Appropriately respond to any past cybersecurity incidents.

III. Online Security Tips

The DOL also outlined a number of security tips, reflecting that participants and beneficiaries also play a large role in the security of their plan accounts. The DOL recommends that users utilize strong and unique passwords for their accounts, add multi-factor authentication to log in, and regularly monitor accounts to guard against the risk of fraud and loss. In addition, the DOL suggests that participants and beneficiaries update their contact information with plans and sign up for account activity notifications to ensure they are notified of any unauthorized account activity. Among the other tips offered, the DOL urges users to avoid public wi-fi networks, remain mindful of phishing attacks, and use up-to-date antivirus software.

Retirement Plan Precautions

Retirement plans are literal treasure troves for cyber criminals – holding large amounts of fund and personal information concerning participants and beneficiaries. Recognizing this concern, the DOL's new cybersecurity guidance may provide a glimpse into future enforcement actions and criteria to assess prudence by fiduciaries in the event of a cyberattack. Plans should consider these tips and insights when engaging new service providers to ensure vendors are taking appropriate precautions to safeguard plan data. They may also wish to revisit current contracts with their present vendors to address any areas where their contracts are silent, as well as consider whether additional measures are necessary to ensure the security and confidentiality of plan data.

Administrators may also wish to review and update their plans' document and retention policies to reflect this new guidance, and review their vendors' policies to confirm if amendments are warranted – with a particular focus on how vendors handle plan data upon expiration or termination of their agreement.

Despite recognizing the important role played by participants and beneficiaries in securing their plan accounts, recommendations regarding cybersecurity education were notably absent from this guidance. Nonetheless, plans may wish to consider passing along the DOL's online security tips to account holders.

If you have any questions, please contact Lawrence J. Finnell, any attorney in our Employee Benefits and Executive Compensation practice or the attorney at the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS