IslerDare PC

Employee Benefits Update

August 13, 2021

DOL Cybersecurity Guidance and Audit Initiative

Executive Summary

The U.S. Department of Labor (the "DOL") recently issued cybersecurity guidance for retirement plans for the first time, which consisted of the following: (i) Cybersecurity Program Best Practices; (ii) Tips for Hiring a Service Provider; and (iii) Online Security Tips. The DOL has already started reviewing the cybersecurity programs of ERISA plan sponsors and fiduciaries as part of a new audit initiative.

This newsletter provides highlights of the DOL's cybersecurity guidance and audit initiative, and provides recommended next steps for plan sponsors and fiduciaries in light of the uptick in cybersecurity inquiries by the DOL and recent incidences involving cybersecurity breaches of benefit plan data.

□–□–□–□–□–□–□–□–□–□–□–□–□–□–□–□–□–□–□

I. Cybersecurity Guidance

The recent DOL guidance comes in three forms:

- Cybersecurity Best Practices: This document is intended to assist plan fiduciaries and recordkeepers responsible for plan-related IT systems and data to manage cybersecurity risks. Some best practices include:
  - Maintaining a formal, well documented cybersecurity program
  - Conducting prudent annual risk assessments
  - Following strong access control procedures
  - Ensuring that any assets or data stored in the cloud or maintained by a third-party service provider are subject to appropriate security reviews and independent security assessments
  - Conducting periodic cybersecurity awareness training
  - Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response
  - Encrypting sensitive data, stored and in transit

- Tips for Hiring a Service Provider: These guidelines provide guidance to plan sponsors and fiduciaries on how to prudently select service providers with strong cybersecurity practices. The recommendations include inquiring about and evaluating the following:
    - The service provider's information security standards, practices and policies, and audit results, compared against industry standards adopted by other financial institutions
    - How the provider validates its practices, and what levels of security standards it has met and implemented
    - Whether the provider experienced past security breaches, what happened, and how the provider responded (these incidents are often reported publicly, so plan sponsors and fiduciaries should consider reviewing news accounts of the service provider's response to the incident)
    - Whether the provider maintains insurance that would cover losses caused by cybersecurity and identity theft breaches, including misconduct by the service provider's own employees or contractor, or a third-party hijacking a plan participant's account
    - The willingness of the service provider to include contract terms requiring ongoing compliance with cybersecurity, clear rules concerning use and disclosure of personal information, responsibility for security breaches, and other key terms addressing exposure to the plan, plan sponsor, and participants

- Online Security Tips: This guidance is intended to help plan participants by providing the following tips to reduce the risk of fraud and loss from their retirement accounts:
    - Registering, setting up and routinely monitoring their online account
    - Using strong and unique passwords
    - Using multi-factor authentication
    - Keeping personal contact information current
    - Closing or deleting unused accounts
    - Being wary of free wi-fi
    - Being aware of phishing attacks
    - Using antivirus software and keeping apps and software current

II. Audit Initiative

Having published this cybersecurity guidance, the DOL is wasting no time in enforcing it through audits. As part of its new audit initiative, the DOL has begun issuing information and document requests relating to plan fiduciaries' cybersecurity practices. These requests ask for information about cybersecurity and information security program policies, procedures, and guidelines that relate to the plan, regardless of whether they are applied by the plan sponsor or by a vendor. The requests also ask for detailed documentation, including security risk assessment reports and service providers' cybersecurity procedures.

III. Recommended Next Steps

We recommend that plan sponsors and fiduciaries take the following steps:

- Review Internal Cybersecurity Programs: Current cybersecurity practices should be routinely analyzed to determine whether they comply with the DOL's recommended best practices and tips. If they do not, appropriate changes should be made to bring the programs and documents in line with the DOL guidance and address any weaknesses that are identified.
- Analyze Service Providers' Cybersecurity Programs and Update Service Contracts: Employers and fiduciaries are responsible for ensuring that service providers are in compliance with the DOL guidance, and we recommend asking service providers to provide information about their cybersecurity procedures. Now would also be a good time to update service provider contacts to include: (i) the service provider's commitment to fully support a DOL audit; (ii) a general obligation for the service provider to comply with the DOL guidance; and (iii) the provisions recommended by the DOL guidance, such as requiring annual third-party audits of security policies and procedures, a commitment to promptly notify the employer/fiduciary of any cyber incident or data breach within a specific amount of time, and maintenance of cyber and other types of insurance.
- Review Participant Messaging around Cybersecurity Awareness: Employers should also consider educating their plan participants about cybersecurity threats and the importance of maintaining robust passcodes and regularly monitoring retirement plan accounts.

To discuss the DOL's cybersecurity guidance, audit initiative, or any other employee benefits matters, please contact any member of our Employee Benefits and Executive Compensation Group below.

IslerDare PC
Your workplace, our insight

1945 Old Gallows Road
Suite 650
Vienna, VA 22182
(703) 748-2690

1111 East Main Street
Suite 1605
Richmond, VA 23219
(804) 489-5507

Andrea I. O'Brien
aobrien@islerdare.com

Vi D. Nguyen
vnguyen@islerdare.com

Jeanne Floyd
jfloyd@islerdare.com

Ashley Hedge
ahedge@islerdare.com