Department of Labor Provides Cybersecurity Guidance

Guidance applies to plan sponsors, service providers, and participants.

June 2021

KEY POINTS

- The DOL recently issued its first-ever cybersecurity guidance for retirement plan sponsors, service providers, and participants.
- The guidance offers a view into the DOL's expectations of what ERISA might require for cybersecurity.
- T. Rowe Price's current cybersecurity practices and preventative measures align with the DOL's guidance.

On April 14, 2021, the Employee Benefits Security Administration (EBSA), the division of the U.S. Department of Labor responsible for enforcing the Employee Retirement Income Security Act of 1974 (ERISA), issued cybersecurity guidance. The guidance, posted to the EBSA website as "Tips for Hiring a Service Provider with Strong Cybersecurity Practices," describes "best practices" and "tips" for plan fiduciaries, plan service providers, and plan participants to address and mitigate the risk of cybersecurity events.

While this long-anticipated sub-regulatory guidance does not carry the weight of a regulation (which is subject to notice and comment), or even the persuasive authority of an Advisory Opinion, it should not be underestimated.

Background

Cybersecurity is a priority for plan sponsors and their service providers. This comes as no surprise, considering recent cybersecurity attacks on individuals, private companies, and governments and given an uptick in fraud events against retirement plan accounts. In addition, recent ERISA litigation alleges that certain plan sponsors and retirement plan service providers allowed unauthorized/fraudulent distributions from participant retirement accounts because of inadequate security practices.

The guidance offers a view into the DOL's expectations of what ERISA might require for cybersecurity.

Advice to Plan Fiduciaries

Although presented as "tips," the DOL's liberal use of the term "should" suggests that plan fiduciaries will use the guidance as a checklist when reviewing a service provider and may increase their inquiries about cybersecurity to their existing service providers.

T. Rowe Price delivers the SOC 2 report annually to plan sponsors (and to prospects upon request) to help demonstrate the security practices of its recordkeeping systems. The SOC 2, a third-party audit report, can facilitate the mapping of identified controls to SPARK's 16 control objectives from its industry best practices for reporting cybersecurity capabilities *(SPARK Institute Industry Best Practices Data Security Reporting)*. As a member of SPARK, T. Rowe Price collaborated with industry peers to establish these industry best practice reporting standards for retirement plan service providers.

Note that T. Rowe Price already meets the cybersecurity criteria described in the "Cybersecurity Program Best Practices for Plan Recordkeepers and Service Providers" guidance.

Plan fiduciaries have obligations under ERISA to make prudent decisions about choosing a service provider. While it's generally understood that there's an obligation to mitigate a plan's exposure to cybersecurity events that could cause a loss of plan assets, plan fiduciaries and service providers might conclude that the DOL intends to investigate cybersecurity practices as part of a DOL audit or enforcement action.

The DOL's list of six "tips" that plan sponsors and responsible fiduciaries "should" follow in fulfilling their duties under ERISA's requirements to "prudently select and monitor" ERISA plan service providers are summarized here:

- Asking about the service provider's security practices, protocols, and audit reports and comparing these systems to industry standards adopted by other financial institutions.
- Inquiring as to how the service provider validates its security controls, including by securing a contractual right to review security system audit results.
- Evaluating the service provider's information security track record, including by reviewing publicly available information on security incidents, other litigation, and legal proceedings related to the service provider's services.
- Asking about whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
- Confirming whether the service provider has sufficient insurance coverage to cover "losses covered by cybersecurity and identity theft breaches," whether caused by internal threats or external threats.
- Incorporating ongoing cybersecurity compliance requirements into service agreements.

The guidance also states that plan fiduciaries "can have much more confidence in the service provider if the security practices of its systems are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality."

Cybersecurity Program Best Practices for Plan Recordkeepers and Service Providers

The DOL also provides guidance to service providers, stating "ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals," and in this guidance, reiterates its position that "responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."

The DOL "prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire." Although the guidance is not a regulatory requirement, it suggests that the DOL expects the following from service providers and might seek confirmation in an investigation or audit:

- 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

The guidance for participants conforms with T. Rowe Price suggested security best practices through the Account Protection Program (APP) and aligns with T. Rowe Price's existing and contemplated anti-fraud and cybersecurity efforts.

to appropriate security reviews and independent security assessments.

- Conduct periodic cybersecurity awareness training.
- Implement and manage a secure system development life cycle (SDLC) program.
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypt sensitive data, stored and in transit.
- Implement strong technical controls in accordance with best security practices.
- Appropriately respond to any past cybersecurity incidents.

Online Security Tips for Participants

The DOL also issued guidance providing tips for participants to reduce the risk of fraud and loss to their retirement accounts. Although it's not clear whether the DOL intended that plan fiduciaries make sure that participants follow this guidance, such as through participant education or communications, the tips reflect standard cybersecurity and anti-fraud practices:

- Register, set up, and routinely monitor your online account.
- Use multi-factor authentication.
- Keep personal contact information current.
- Use strong and unique passwords.
- Close or delete unused accounts.
- Be wary of free Wi-Fi.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.

Next Steps

T. Rowe Price will continue to monitor the DOL's guidance. Please contact your T. Rowe Price representative if you have any questions.

T.RowePrice®

T. Rowe Price Retirement Plan Services, Inc.
T. Rowe Price Investment Services, Inc.
T. Rowe Price Associates, Inc.

CCON0097597
202106-1667714