

UPDATE:
DOL Cybersecurity Guidance and
SECURE ACT 2.0

Presented By:
Elizabeth Goldberg · Heather Stone Fletcher · Anne Greene

DOL Cybersecurity Guidance

Litigation Background

- ▶ There have been increasing amounts of litigation over alleged identity theft and fraudulent distributions.
- ▶ Several lawsuits have been filed recently against plan sponsors, plan fiduciaries, administrators, and recordkeepers after thieves hacked plan participants' personal information and used that information to drain participants' 401(k) plan accounts.
 - ▶ Prior court precedent is relatively favorable to plan fiduciaries, but there is some concern that the law will become less favorable as additional cases (with worse facts) are heard.
- ▶ There has also been increased litigation alleging that plan fiduciaries have failed to properly secure plan data.

Significant Risks

- ▶ This area presents significant risks for plan fiduciaries
 - ▶ Retirement plans present an attractive opportunity for criminals to obtain the most sensitive of personal information
 - ▶ Plaintiffs' bar continues to be exceptionally active presenting novel theories of fiduciary liability
 - ▶ Proactive engagement of providers and security personnel and education and training
 - ▶ DOL has begun enforcement initiatives focusing on cyberliability issues
 - DOL has criminal, as well as civil, investigatory authority

The DOL Issues First-of-Its-Kind Cybersecurity Guidance

- ▶ On April 14, 2021, the DOL issued three pieces of subregulatory guidance addressing the cybersecurity practices of retirement plan sponsors, their service providers, and plan participants, respectively.
- ▶ Is the guidance enforceable?
 - ▶ While this subregulatory guidance is not entitled to deference—and arguably does not even have the persuasive authority of an Advisory Opinion—it provides a window into the DOL’s expectations for a “prudent” plan fiduciary’s cybersecurity practices.
- ▶ The DOL has begun an enforcement effort in this area.

New Guidance

- ▶ Each of the three new pieces of guidance addresses a different audience.
 - ▶ *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* provides guidance for plan fiduciaries when hiring a service provider, such as a recordkeeper, trustee, or other provider that has access to a plan’s nonpublic information.
 - ▶ *Cybersecurity Program Best Practices* is a collection of best practices for recordkeepers and other service providers, that may be viewed as a reference for plan fiduciaries when evaluating service providers’ cybersecurity practices.
 - ▶ *Online Security Tips* contains online security advice for plan participants and beneficiaries.

Analysis of Plan Sponsor Guidance

Tips for Hiring a Service Provider

- ▶ *Tips for Hiring a Service Provider* outlines factors for “business owners and fiduciaries” to consider when selecting retirement plan service providers.
- ▶ While the plan fiduciary may have a variety of fiduciary obligations with respect to potential cybersecurity events, one of its most important responsibilities relates to properly ensuring that plan service providers have adequate safeguards to mitigate cybersecurity risks.
- ▶ This is because the plan’s service providers normally have the most direct access to plan assets and are the most vulnerable to permitting fraudulent distributions.

Six Tips for Hiring a Service Provider

1. Ask about the service provider's data security standards, practices, and policies and audit results and benchmark those against industry standards.
2. Analyze the service provider's security standards and security validation practices.
3. Evaluate the service provider's track record in the industry.
4. Ask about past security events and responses.
5. Confirm that the service provider has adequate insurance coverage for losses relating to cybersecurity and identity-theft events.
6. Ensure that the services agreement between the plan fiduciary and the service provider includes provisions requiring ongoing compliance with cybersecurity standards.

Tips for Hiring a Service Provider - Comments

- ▶ Conspicuously absent from this guidance is a clear statement regarding a fiduciary's obligations with respect to current service providers.
- ▶ Plan fiduciaries could consider using the *Tips for Hiring a Service Provider* when preparing requests for information and requests for proposal.
- ▶ When entering into a new agreement, the plan fiduciary could engage in meaningful negotiations over the terms of the agreement discussed in this guidance (e.g., cybersecurity, protection and use of confidential data, insurance coverage).

12 Cybersecurity Best Practices

Practices 1-6

1. Have a formal well-documented cybersecurity program
2. Conduct prudent annual risk assessments
3. Have a reliable annual third-party audit of security controls
4. Clearly define and assign information security roles and responsibilities
5. Have strong access-control procedures
6. Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate safeguards

Practices 7-12

7. Conduct periodic cybersecurity training
8. Implement and manage an SDLC program
9. Have an effective business resiliency program addressing BCDR and incident response
10. Encrypt sensitive data, stored and in transit
11. Implement strong technical controls in accordance with best practices
12. Appropriately respond to any past cybersecurity incidents

Online Security Tips - Advice to Reduce Risk

Nine Tips for Participants

1. Register, set up, and routinely monitor account
2. Use strong and unique passwords
3. Use multifactor authentication
4. Keep personal information current
5. Close or delete unused accounts
6. Be wary of free Wi-Fi
7. Beware of phishing attacks
8. Use antivirus software and keep apps and software current
9. Know how to report ID theft/incidents

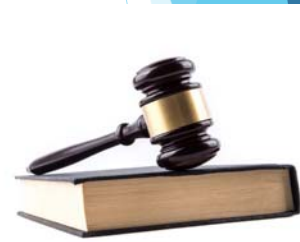
Administrator Considerations

- ▶ Encouraging participants and beneficiaries to follow these tips may help mitigate exposure to cybersecurity threats
 - ▶ Multiprong education campaign:
 - Window pop-ups
 - Emails and letters
 - Videos
 - SPDs

SECURE Act 2.0

SECURE Act

- ▶ Setting Every Community Up for Retirement Enhancement Act of 2019
- ▶ Bill was passed and signed into law on December 20, 2019
- ▶ Most significant retirement plan legislation since Pension Protection Act of 2006
- ▶ Goal was to expand and preserve retirement savings
- ▶ Affects most retirement plan sponsors and individual retirement account and annuity (IRA) providers, plan participants and IRA owners, and their beneficiaries
- ▶ Changes have had a significant impact on retirement, estate, and tax plans in both the employer-sponsored retirement plan and retail retirement market



Key SECURE Act Changes

- ▶ Eliminates age 70½ limit for making traditional IRA contributions
- ▶ Raised age for taking required minimum distributions to April 1 of the year following year in which individual reaches age 72 (up from age 70½)
- ▶ Added exception to 10% early distribution penalty for “qualified birth or adoption distribution” of up to \$5,000 if certain conditions are met
- ▶ Provides a new safe harbor that defined contribution plan fiduciaries can rely on in selecting lifetime income investment providers to make available as an investment option or a component of an investment option under the plan
- ▶ Allows plan sponsors to permit participants to transfer lifetime income investment to an eligible retirement plan or take a distribution annuity contract

15

Key SECURE Act Changes (cont.)

- ▶ Eliminates stretch distribution for most beneficiaries; requires distributions within 10 years of IRA owner/plan participant’s death for most beneficiaries other than “eligible designated beneficiaries”
- ▶ Requires 401(k) plans to extend participation—solely for purposes of making elective deferrals—to any part-time employee who has worked at least 500 hours in each of the three immediately preceding consecutive 12-month periods
- ▶ Requires plans to issue annual benefit statements that include an estimate of the monthly income a participant could receive in retirement if a QJSA or an SLA were purchased
- ▶ Reduces from age 62 to age 59½ the earliest age an employee can receive in-service retirement benefits from a pension plan

16

Key SECURE Act Changes (cont.)

- ▶ Increases qualified automatic contribution arrangement safe harbor rate cap to avoid nondiscrimination testing from 10% to 15% after participant's first year
- ▶ Eliminates the annual notice requirement for safe harbor 401(k) plans that avoid nondiscrimination testing by providing a minimum 3% nonelective contribution
- ▶ Permits a 401(k) plan to elect into the 3% nonelective safe harbor at any time up until 30 days before the close of the plan year
- ▶ Provides nondiscrimination testing relief with respect to certain closed or "soft-frozen" defined benefit plans
- ▶ Directs the IRS and DOL to modify annual retirement plan reporting rules to permit certain individual account plans or defined contribution plans to file a consolidated Form 5500
- ▶ Increases penalty for failing to file a Form 5500 from \$25 to \$250 per day and increases penalty cap from \$15,000 to \$150,000

17

SECURE Act 2.0

- ▶ US House Representatives Richard Neal and Kevin Brady recently introduced the Securing a Strong Retirement Act
- ▶ Commonly referred to as SECURE Act 2.0, the bill includes changes that would further encourage plan adoption and retirement savings and provide solutions to longstanding operational problems
- ▶ On May 5, 2021, the House Ways and Means Committee unanimously approved SECURE Act 2.0 (H.R. 2954)
- ▶ On June 23, 2021, the House Committee on Education and Labor held a hearing on SECURE 2.0
- ▶ Complimentary and competing proposals have been introduced in the Senate



18

Key SECURE Act 2.0 Changes

- ▶ Automatic enrollment features would be required for new plans
- ▶ Allows employers to treat employee student loan payments as if they were elective deferrals to the 401(k) plan and make “matching” contributions to the participant’s 401(k) account
- ▶ Raises the catch-up contribution limit for individuals age 62, 63 and 64
- ▶ Expands a plan’s ability to self-correct under EPCRS, and provides qualification safe harbors for other corrections
- ▶ Increases RMD beginning date from age 72 to age 75 (staged progression)

19

Key SECURE Act 2.0 Changes (cont.)

- ▶ Creates a national online database of lost accounts to help employees find savings held at former employers
- ▶ Allows 403(b) plans to invest in collective investment trusts (CITs), and allows for the creation of multiple employer 403(b) plans
- ▶ Addresses issues related to QLACs
- ▶ Reduction of the period of service requirements for part-time employees
- ▶ Offers a new credit for businesses with 100 or fewer employees that would offset up to \$1,000 of employer contributions per employee (would phase out over five years)

20

Questions?


Thank You!

21

Due to updates on the polling site, a Thank You for texting message will no longer be sent.

Texting in for CE is only allowed one time but is received and will be updated to your account normally within 72 hours

22



To Claim CE for this meeting:
Text # **22333**
Use session ID **74132** {space}
and then your ASPPA ID#
(See sample of phone picture)
Please text within 48 hours of attendance