A Trillion Dollar Target – 401(k) Plan Cybersecurity Risk

CLE Seminar for In-House Counsel Webinar Series
2021

Course Overview

- The Road to DOL Guidance
- DOL Cybersecurity Guidance
- Plan Sponsor and Fiduciary Next Steps
- Questions

The Road to DOL Guidance

The Road to DOL Guidance

Stakes & Sources of Risk

Retirement Plans Provide a Big Target

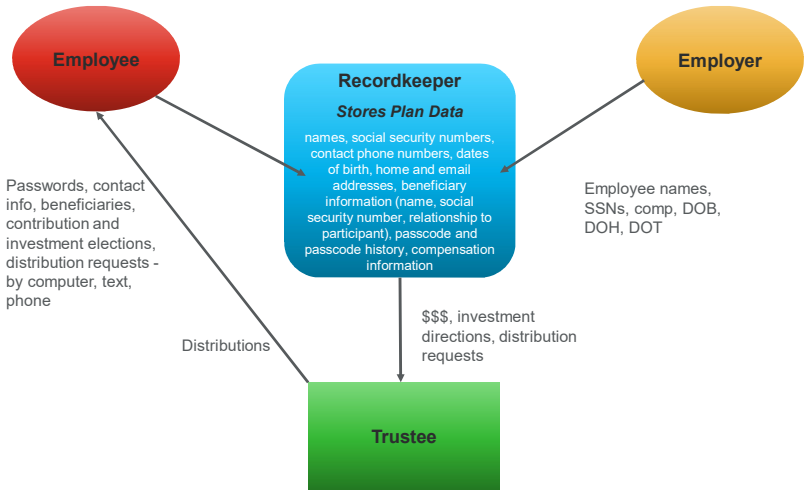
- ***Money*** -- In 2020, U.S. retirement assets totaled $28.7 trillion, with 401(k) plans accounting for $5.6 trillion.
- ***Data*** -- Plan data generally includes participant names, social security numbers, contact phone numbers, dates of birth, home and email addresses, beneficiary information (name, social security number, relationship to participant), passcode and passcode history, compensation information, and other personal identifying information.

Technology

- As technological capabilities increase, so do cybersecurity threats, particularly with respect to defined contribution retirement plans, such as 401(k) plans.
- Increases in mobile access, network connectivity, third-party vendors, and service providers create more entry points to plan assets and data.

The Road to DOL Guidance

Entry Points/Flow of Information



The Road to DOL Guidance

The Threat is Real - Plans are Being Targeted Every Day

June 2016 - $2.6 million was taken from the retirement accounts of 58 city of Chicago employees via fraudulent loans. The hackers used employees' personal information and set up web profiles that allowed them to take out loans from the retirement accounts.

December 2017 - A scheme targeting individual 401(k) accounts, potentially at multiple recordkeepers, resulted in a lawsuit by the U.S. Attorney's office in Colorado to recover from the individual criminals over $500,000 in fraudulently obtained distributions. According to the lawsuit, unauthorized individuals used participant's personal information to create online profiles and withdraw funds from retirement accounts.

April 2018 - A major recordkeeping firm notified certain plans that imposters posing as plan participants had requested plan distributions and attempted to gain access to plan assets with varying degrees of success.

June 2019 - A New Mexico state employee pension plan notified approximately 100,000 members of a breach of their personal information via a stolen unencrypted laptop.

The Road to DOL Guidance

The Threat is Real - Agency Penalties

- Vendors have avoided reporting hacks and attempted hacks.
- March 2021 – Securities and Exchange Commission fined GWFS Equities, Inc. (an affiliate of Empower Retirement) $1.5 million for not properly reporting attempts to hack into customer individual retirement accounts over a three-year period.
  - Empower is the second largest retirement plan administrator in the United States with more than 12 million participant accounts and $1 trillion in assets.

The Road to DOL Guidance

The Threat Is Real - Rise in Participant Litigation

- Participants are increasingly trying to hold plan fiduciaries responsible for losses due to hacks and cybersecurity failures.
- *Berman v. Estee Lauder Inc.,* Civil Action No 3:19-cv-06489 (N.D. Cal. 2019) (unpublished case, reportedly settled in March 2020)
  - Participant sued plan fiduciaries alleging that her $90,000 401(k) plan account with Alight Solutions (formerly Hewitt Associates) was reduced to $3,800 by a series of three unauthorized withdrawals.
- *Leventhal v. MandMarblestone Grp.*, Civil Action No. 18-cv-2727 (E.D. Pa. 2019)
  - Plan, employer and participant sued plan advisor and custodian after criminals obtained a copy of the participant's withdrawal form and used it to make additional electronic withdrawals from the participant's account, depleting it from $400,000 to $0.
- *Barnett v. Abbott Laboratories, et. al.,* Civil Action No. 20-cv-02127 (N.D. Ill. 2020)
  - Participant sued plan fiduciaries alleging that $245,000 was transferred from her plan account because Alight's procedures improperly allowed an unauthorized person to access her account, change her password and add a new bank account number.
- *Mandli v. American Trust Company*, Case No. 21-cv018 (W.D. Wis. January 2021)
  - Participant and plan sued recordkeeper alleging that $124,000 was distributed from plan account as a result of distribution forms sent to email and mail addresses not on file with the recordkeeper.

The Road to DOL Guidance

Absence of Guidance

- Until last month, there was no comprehensive federal regulatory guidance governing cybersecurity for retirement plans or their service providers.
  - ERISA is silent on data protection of electronic records.
  - However, ERISA's general fiduciary duties include prudent oversight of plan administration, and selection and monitoring of service providers.
  - Damages can result from breaches of these fiduciary duties, including personal liability of the fiduciary.

The Road to DOL Guidance

Absence of Guidance

- In November 2016, the ERISA Advisory Council issued a report called "Cybersecurity Considerations for Benefit Plans."
  - Plan sponsors and fiduciaries should consider cybersecurity in safeguarding assets.
  - Personal data and asset information should be specifically considered when implementing cybersecurity.
  - Not only should plan sponsors and fiduciaries consider internal safeguarding mechanisms, but they should also develop strategies for selecting and retaining service providers.
- The council encouraged education on cybersecurity and referred to industry experts for potential approaches to manage risks.

The Road to DOL Guidance

GAO Report

- In February 2019, the House and Senate Health, Education, Labor, and Pensions Committees requested the U.S. Governmental Accountability Office examine the cybersecurity of the retirement system, noting that digital pathways between the plans and their service providers are "*a tempting target for criminals who could hack into plans and individuals' accounts to access information, commit identity fraud, and steal retirement savers' nest eggs.*"
- In February of this year, the GAO issued a report concluding that the need to protect administrative systems for defined contribution plans has become paramount, and recommending to the Department of Labor that it:
  - formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in DC plans; and
  - establish minimum expectations for addressing cybersecurity risks in DC plans.

DOL Cybersecurity Guidance

DOL Cybersecurity Guidance

- Released Online April 14, 2021
- Sub-regulatory Guidance
- Three Topics
  - Tips for Hiring a Service Provider with Strong Cybersecurity Practices
  - Cybersecurity Program Best Practices
  - Online Security Tips

DOL Cybersecurity Guidance

Tips for Hiring a Service Provider

- Directed at plan sponsors and other plan fiduciaries
- Fiduciary obligation to prudently select and monitor service providers (DOL Reg. § 2550.404a-5(f))
- DOL Guidance: "Plan sponsors ***should*** use service providers that follow strong security policies"
- Key Components
  - Due Diligence
  - Contracting

DOL Cybersecurity Guidance

Tips for Hiring a Service Provider

Due Diligence
What are the provider's security standards, practices and policies, and audit results and how do they compare to industry standards adopted by other financial institutions?
How does the provider validate its practices, and what level of security standards has it met and implemented?
What is the provider's track record in the industry?
Are there insurance policies that would cover losses caused by cybersecurity and identity theft breaches?

DOL Cybersecurity Guidance

Tips for Hiring a Service Provider

Contracting
"Make sure" contract requires ongoing compliance with cybersecurity and information security standards
"Beware" of limitations of liability
Try to negotiate contract terms that enhance cybersecurity protection for the plan and participants, such as: • Information Security Reporting • Clear Use & Sharing of Information Terms • Notification of Cybersecurity Breaches • Compliance with Record Retention & Destruction, Privacy & Information Security Laws

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- Directed at recordkeepers and other plan service providers
- Service providers ***should***:

• Have a formal, well documented cybersecurity program	• Conduct periodic cybersecurity training
• Conduct prudent annual risk assessments	• Implement & manage a SDLC program
• Have a reliable annual third party audit of security controls	• Adopt an effective business resiliency program
• Clearly define & assign information security roles & responsibilities	• Encrypt sensitive data stored & in transit
• Have strong access control procedures	• Implement strong technical controls
• Implement appropriate cloud securities	• Appropriately respond to cybersecurity incidents

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- A Formal, Well Documented Cybersecurity Program
  - Identify risks
  - Protect the assets
  - Detect and respond to cybersecurity events
  - Recover from cybersecurity events
  - Appropriately disclose the event
  - Restore normal operations

- Prudent Annual Risk Assessment
  - Identify, estimate, and prioritize information system risks

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- A Reliable Annual Third Party Audit of Security Controls
  - EBSA would "***expect to see***"
    - Audit reports and other analyses and reviews
    - Documented corrections of any identified weaknesses
- Clearly Defined & Assigned Information Security Roles & Responsibilities
  - To be effective, program ***must*** be managed at the senior executive level (ex. CISO) and executed by qualified personnel

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- Strong Access Control Procedures
  - Authentication
  - Authorization
- Assets or Data Stored in a Cloud or Managed by a Third Party Service Provider are Subject to Appropriate Security Reviews and Independent Security Assessment
  - Plan provider must conduct diligence on cloud provider
  - Plan provider should ensure guidelines and contractual protections meet certain minimum standards

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- Cybersecurity Awareness Training
  - At least annually for *all* employees
  - Updated to reflect risks identified by the most recent risk assessment
  - Identity theft should be a key topic
- Secure System Development Life Cycle (SDLC) Program
  - Security assurance activities (ex. penetration testing, code review, and architectural analysis) should be an integral part of system development efforts

DOL Cybersecurity Guidance

Cybersecurity Program Best Practices

- Encryption of Sensitive Data
  - Protect the confidentiality and integrity of data at rest or in transit
- Strong Technical Controls Implementing Best Security Practices
  - Hardware, software, and firmware components
- Responsiveness to Cybersecurity Incidents or Breaches
  - Notify law enforcement and appropriate insurance carrier
  - Investigate incident
  - Help plans and plan participants prevent or mitigate injury
  - Honor contractual and legal obligations
  - Address the source of the breach

DOL Cybersecurity Guidance

Online Security Tips

- Directed at plan participants

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

DOL Cybersecurity Guidance

Open Questions

- What party is responsible for a breach?
- Does ERISA preempt state cybersecurity and data privacy laws?
- Is data about retirement plan participants a plan asset?
  - Issue working through the court systems
- What impact does the guidance have on health plan cybersecurity?

This page intentionally left blank.

Plan Sponsor and Fiduciary Next Steps

Plan Sponsor and Fiduciary Next Steps

Review Current Service Provider Practices

- Communicate with recordkeeper and other plan service providers
  - How does the provider use, and does it share, participant data?
  - Request details regarding existing cybersecurity protocols
  - SOC 2 Report
  - What additional actions, if any, is the service provider taking in light of the DOL's guidance?

Plan Sponsor and Fiduciary Next Steps

Review Service Provider Agreement

- Are there provisions in the governing contract regarding the service provider's cybersecurity obligations?
- Consider trying to amend the contract to:
  - Impose an obligation on the service provider to use an industry standard level of care
  - Provide indemnification for cybersecurity issues
  - Tailor exculpatory clauses
- Service provider may not be willing to amend the contract in a manner that increases its contractual liability

Plan Sponsor and Fiduciary Next Steps

Fiduciary Protections

- Document sponsor's review of current service provider practices and any attempted contract negotiations
- Review fiduciary liability insurance and fidelity bond coverage
- Consider obtaining cybersecurity insurance
  - Beware of carve outs under the policy
- When seeking a new service provider - revise request for proposal (RFP) questions to reflect DOL guidance

Plan Sponsor and Fiduciary Next Steps

Participant Communications

- Educate - distribute DOL participant tips to employees
- Review and revise summary plan description (SPD)?
  - Participant obligation to keep the employer up to date on life events (marriage, divorce, change in address, etc.)
  - Include a reference to, or incorporate, the DOL's tips on cybersecurity?
- Other communications or employee cybersecurity training?

Questions?

大成DENTONS

Thank you