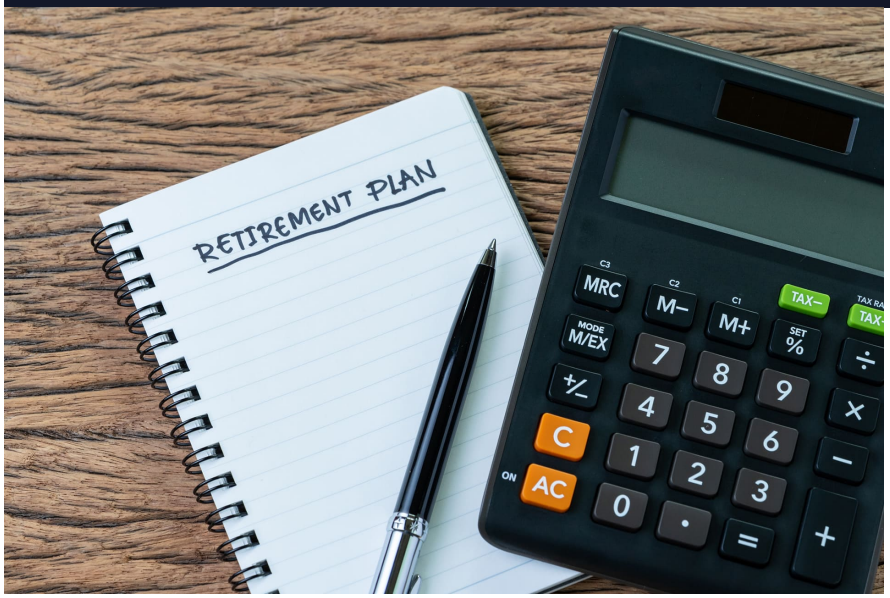
BARNES & THORNBURG LLP



ALERTS

EBSA's Cybersecurity Guidance For Retirement Plans

April 30, 2021

Highlights

The EBSA's cybersecurity guidance provides a road map for ERISA plan fiduciaries to hedge against cybersecurity risks to retirement plans

Service provider contracts should be reviewed to incorporate cybersecurity provisions aligned with EBSA's guidance

Plan fiduciaries should communicate EBSA's guidance to participants so they can take steps to protect their retirement account security

On April 14, 2021, the U.S. Department of Labor's Employee Benefits Security Administration (EBSA) issued guidance on cybersecurity for ERISA pension benefit plans, in response to the Government Accountability Office's request for suggestions on how benefit plan officials should hedge against cybersecurity risks threatening plan assets and plan participant data.

The EBSA guidance elevates cybersecurity to priority status for those who manage retirement plans and is divided into three parts: 1) plan sponsors and fiduciaries, 2) record-keepers and other service providers,

RELATED PEOPLE

Mina Amir-Mokri
Partner
Chicago

P 312-214-4804
F 312-759-5646
mina.amir-mokri@btlaw.com

RELATED PRACTICE AREAS

Benefits and Compensation
Corporate
COVID-19 Resources
Labor and Employment

and 3) plan participants.

Plan Sponsors and Fiduciaries

To fulfill their duties to the ERISA retirement plans they oversee, fiduciaries and plan sponsors must take the proper due diligence steps to identify and hedge against cybersecurity risks. Data theft and other cyberattacks are increasingly a reality, and likely fertile ground for the plaintiffs' bar. The EBSA's recommendations are aligned with cybersecurity policies and procedures typically adopted by many organizations. The guidance provides a roadmap for ERISA plan fiduciaries to mitigate against both cybersecurity threats and the threat of a fiduciary breach claim for failure to protect participants' privacy and account security.

Key guidance to plan sponsors and fiduciaries includes hiring service providers with strong cybersecurity systems, and the importance of selecting and monitoring such service providers prudently. Best practices include:

- Conduct a background check on the service provider from generally available public information, including press reports and litigation records
- Ask the prospective service provider about whether and the extent to which they have experienced cybersecurity breaches, how they responded, and the measures taken since to mitigate against such breaches
- Assess the service provider's cybersecurity systems and standards, practices and policies
- Review results of past outside independent audits and responses to prior cybersecurity breaches, including subsequent mitigation measures adopted
- Review insurance policies that cover losses, including identity theft, from internal and external cybersecurity breaches
- Ensure service provider agreements include:
    - Ongoing compliance with cybersecurity and information security standards
    - A requirement that an annual audit of compliance with cybersecurity and information security standards, policies and procedures be conducted by an outside independent auditor
    - No limits on the service provider's responsibility for cybersecurity breaches
    - A right to review audit results
    - Confidentiality covenants with regard to private information and protection against unauthorized access and disclosure of private information

- A requirement that the service provider notify the plan sponsor of any cyber incident within a specified time period after the incident
- A covenant that the service provider will actively investigate or cooperate in the investigation of any cyber incident, and take proper remedial measures

Record-Keepers and Other Service Providers

The guidance for record-keepers and other service providers details general cybersecurity program best practices to protect participant data and ensure proper mitigation of cybersecurity risks, including:

- Implementing a formal, well-documented cybersecurity program
- Performing annual risk assessments to identify and prioritize information system risks and a plan to manage the identified risks
- Holding annual outside independent audits of cybersecurity system controls, including breach testing reports and documented corrections of any vulnerabilities identified in the audit
- Designating information security roles and responsibilities
- Accessing control procedures
- Performing proper security reviews and independent security assessments of cloud service providers or other third party providers
- Holding cybersecurity awareness training, updated periodically for current risk assessment
- Implementing and managing a secure system development life cycle program
- Implementing a business resiliency program to address business continuity, disaster recovery, and incident response
- Encrypting sensitive data at all times, both stored and in transit
- Implementing strong technical controls in accordance with best security practices
- Creating and implementing a proper response plan of action to any cybersecurity incidents

Plan Participants

The EBSA has also provided guidance to plan participants to reduce the risk of loss to their retirement accounts. It recommends that plan participants:

- Set up and routinely monitor online accounts
- Create strong passwords, changing them every 120 days
- Use multi-factor authentication to verify identity
- Keep personal contact information current so they can promptly be contacted by the plan sponsor in case of an incident
- Close or delete unused accounts to reduce online presence
- Use wireless network protocols with care
- Beware of phishing, which has increased significantly during the COVID-19 pandemic
- Use antivirus software and timely install updates
- Report identity theft and other cybersecurity incidents to the plan, but also to the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), when necessary

Action Steps for Plan Fiduciaries

The EBSA's guidance asserts cybersecurity should be a top priority for ERISA plan fiduciaries in fulfilling their duties to the plans they oversee and suggests they:

- Review their current cybersecurity oversight process and internal controls in light of EBSA's guidance
    - Update fiduciary training to include EBSA guidance
    - Implement procedures by which cybersecurity diligence and compliance are documented
- Update plan documents as necessary, and prepare disclosures to communicate cybersecurity protective measures to inform participants of the steps they should take to protect their identity and account information
- Review the cybersecurity practices and controls of their service providers
- Amend service provider agreements as necessary to align them with EBSA's cybersecurity guidance

To obtain more information regarding this alert, contact the Barnes & Thornburg attorney with whom you work or Mina Amir-Mokri at 312-214-4804 or mina.amir-mokri@btlaw.com.

legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own lawyer on any specific legal questions you may have concerning your situation.