akerman

Blog Post

ERISA Plan Sponsors – Watch Your Participants' Data! DOL Issues New Cybersecurity Guidance for Retirement Plans

April 19, 2021

By Beth Alcalde and Elizabeth F. Hodge

In response to a recent General Accounting Office (GAO) report recommending federal guidance to mitigate cybersecurity risks in retirement plans and to respond to ever-increasing cyber threats to plan participant data and plan assets, the DOL's Employee Benefits Security Administration (EBSA) published its first cybersecurity guidance for plan sponsors, plan fiduciaries, record keepers, and plan participants of ERISA-covered retirement plans. The guidance issued on April 14, 2021 address the following three topics:

- Cybersecurity program best practices for services providers;
- Plan sponsor tips for evaluating service providers' cyber security practices; and
- Online security tips for plan participants.

On balance, this week's guidance is helpful to plan participants who want to take an active role in doing their part to ensure their data is secured. But from the perspective of employer plan sponsors and other ERISA plan fiduciaries, the guidance provides much food for thought. Certainly, employers are now on notice regarding their heightened obligations to

Related People

Beth Alcalde
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Employee Benefits and ERISA Litigation
Employee Benefits and Executive Compensation
Labor and Employment

Related Offices

West Palm Beach

HR Defense

Akerman Perspectives on the Latest Developments in Labor and Employment Law

Visit this Akerman blog

protect the privacy and security of plan participants' information and retirement accounts, and those who have historically taken a more narrow focus on fiduciary duties are wise to layer cybersecurity and general data privacy advisors into their legal resource teams.

The February 2021 GAO report had recommended that the DOL formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks in defined contribution plans. At the time GAO issued its report, the DOL did not state whether it agreed or disagreed with the concept that a plan fiduciary has a responsibility to mitigate cybersecurity risk. Now, in the announcement accompanying release of the new guidance, the DOL unequivocally answers the question in the affirmative.

This week's guidance confirms that ERISA requires plan fiduciaries to take appropriate steps to identify and mitigate the risks posed by internal and external cybersecurity threats in a retirement plan context. This is a noteworthy, functional expansion of ERISA's fiduciary framework. Although the ERISA plaintiff's bar has not gained significant ground in the cybersecurity litigation space, there is no doubt that cyberattacks and data theft considerations are increasingly high stakes issues. Fortunately, the new DOL guidance creates a substantive roadmap for plan sponsors and service providers that wish to proactively address these matters.

Below we summarize the three guidance documents released by the EBSA. Many of the concepts draw upon generally-recognized cybersecurity best practices and recommendations. As such, operational leaders at companies sponsoring defined contribution plans may recognize EBSA's recommendations as being similar to cybersecurity policies and procedures they have already implemented in connection with their business

operations. But other ERISA plan fiduciaries who have not had a professional need to concern themselves with the ever-changing cybersecurity landscape may find this guidance less familiar. In such cases, we expect that fiduciaries will seek training by advisors who are able to address the unique overlap between ERISA fiduciary responsibilities and retirement plan compliance topics, with the appropriate and applicable cybersecurity and privacy frameworks.

Cybersecurity Program Best Practices

EBSA offers the following best practices for recordkeepers and other service providers responsible for plan-related information systems and for plan fiduciaries making prudent decisions about the services providers they engage.

- Have a formal, well documented cybersecurity program.
- Conduct prudent annual risk assessments to identify and prioritize information system risks. A plan to manage the identified risks should be part of the risk assessment.
- Have a reliable annual third-party audit of security controls. Plan fiduciaries, recordkeepers, and service providers should pay particular attention to the activities that EBSA says it would expect to see as "part of its review of an effective audit program." These include audit reports and penetration testing reports by third parties and documented corrections of any weaknesses identified in a third-party analysis.
- Clearly define and assign information security roles and responsibilities. EBSA expects the cybersecurity program to be managed by a senior level executive with appropriate qualifications, such as the Chief Information Security Officer.
- 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 to appropriate security reviews and independent security assessments. EBSA says that organizations must understand the security posture of the cloud service provider (CSP) in order to make sound decisions using the CSP.

- As mentioned above, conduct periodic cybersecurity awareness training. The training should be updated to reflect risks identified in the most current risk assessment. EBSA recommends that identity theft be a key component of the training as that is a leading cause of fraudulent distributions. For example, employees tasked with retirement plan-related responsibilities should be trained to spot individuals falsely posing as authorized plan officials, fiduciaries, participants or beneficiaries.
- Implement and manage a secure system development life cycle program.
- Have an effective business resiliency program (BRP) addressing business continuity, disaster recovery, and incident response. A BRP allows an organization to adapt to disruptions and continue operations, including the ability to safeguard participants' information and accounts.
- Encrypt sensitive data at rest and in transit.
- Implement strong technical controls in accordance with best security practices.
- Appropriately respond to any cybersecurity incidents.

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

EBSA expects plan sponsors to use service providers that have robust cybersecurity practices. To help plan sponsors and fiduciaries prudently select and monitor such service providers, EBSA offers the following recommendations:

- Plan sponsors should ask about the service provider's information security standards, practices and policies, and audit results, and

compare them to the industry standards adopted by other financial institutions. Service providers should follow a recognized standard for information security and use third-party auditors to review and validate cybersecurity practices. Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Plan sponsors should insist on contract provisions that give them the right to review audit results demonstrating compliance with the standard.

- Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.
- Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
- Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account). Plan sponsors should contractually require service providers to carry policies that will cover cyber incidents such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage. Policy limits should be appropriate for the exposure.
- When contracting with a service provider, the plan sponsor should make sure that the contract requires ongoing compliance with cybersecurity and information security standards. Plan sponsors should also try to include terms that:

- Require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.
- Obligate the service provide to maintain the confidentiality of private information, prevent the use or disclosure of confidential information without written permission, and meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse.
- Require the service provider to notify the plan sponsor of any known or suspected cyber incident, including specifying how quickly the service provider must give such notice, to whom such notice is to be provided, and what information is to be included in the notice. The service provider should also agree to cooperation in investigating the incident and remediating the cause of the breach.
- The service provider will comply with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information, including but not limited to, breach notification laws.

Online Security Tips

While plan fiduciaries have an obligation to take precautions to mitigate cybersecurity risks, EBSA also created guidance for plan participants that offers ways in which they can reduce the risk of fraud or loss to their retirement accounts. Specifically, EBSA recommends that plan participants:

- Register, set up, and routinely monitor online accounts to spot suspicious activity involving your accounts.

- Use strong and unique passwords, changing them every 120 days.
- Use multi-factor (or two-factor) authentication to verify your identity.
- Keep personal contact information current so the plan sponsor can promptly reach you if there is a problem.
- Close or delete unused account to reduce your online presence.
- Beware of free Wi-fi networks. They present security risks and may end up costing plan participants in the long run.
- Watch for phishing attacks, which have increased significantly during the COVID-19 pandemic.
- Use anti-virus software and timely install updates to apps and software.
- In addition to what we would expect to be a reporting framework within the plan itself, in certain cases consider reporting identity theft and cybersecurity incidents to the FBI and the Department of Homeland Security.

These tips are well-timed given that plan participants are working remotely and interfacing with plan recordkeeping sites from a wide range of personal computing devices on an incredible scale. In fact, many participants expect to have mobile account access and the ability to provide remote elective directions to plan custodians. Prudent plan sponsors should consider periodically communicating online security tips to their participants, just as they provide general retirement fund growth tips or remind participants about available matching funds.

Key Takeaways

The DOL has now confirmed that ERISA fiduciaries have an obligation to take affirmative steps to mitigate the risk to plan participants and plan assets posed by cyber threats. As such, plan fiduciaries and sponsors should review the guidance, assess how

their current cybersecurity practices and those of their recordkeepers and service providers compare with the EBSA recommendations, consider service provider contract and plan document amendments as appropriate, and develop a plan to implement the recommendations. Of particular importance, fiduciary training should be considered as part of any such plan. Fiduciaries, sponsors, recordkeepers, and service providers should also document their compliance efforts as it seems certain the DOL and other regulators will, increasingly over time, expect ERISA plan sponsors and fiduciaries to substantiate their cybersecurity compliance training, procedures, and participant disclosure approaches.

For assistance with these or other ERISA issues, contact your Akerman lawyer.
