DOL Guidance on Fiduciary Cybersecurity for Employee Benefit Plans

April 20, 2021

4-Minute Read

The U.S. Department of Labor (DOL) recently announced new guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity. Although much of the guidance is intended to protect retirement benefits, the rules also generally apply to health and welfare benefits subject to the Employee Retirement Income Security Act of 1974 (ERISA). The guidance comes in three forms: 1) Tips for Hiring a Service Provider, 2) Cybersecurity Best Practices and 3) Online Security Tips. Plan sponsors, fiduciaries, and third-party service providers should seriously evaluate their current cybersecurity protocol and processes in order to prevent regulatory and civil liability in connection with cybersecurity breaches affecting employee benefit plans.

Tips for Hiring a Service Provider

ERISA requires that plan sponsors exercise prudence in the selection of service providers, which includes an evaluation of the provider's cybersecurity practices. Plan administration often involves the delegation of administrative responsibility to third parties that often maintain plan records, participant data and other confidential information. When engaging a service provider, the DOL encourages plan sponsors to request information regarding the service provider's security standards, practices and policies, and to audit results by comparison to the industry standards. Further, service providers should not be considered for engagement if they fail to follow a recognized standard for information security.

ERISA requires that plan fiduciaries implement a diligence process for evaluating potential service providers as a matter of prudence. Accordingly, the DOL guidance encourages fiduciaries to evaluate the service provider's track record in the industry, including public information regarding information security incidents and legal proceedings related to vendor's

services. Prudence may also require that the service provider confirm the existence of 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 information). Additionally, the terms of the contract with the service provider should have provisions to address the following.

- **Clear provisions on the use and sharing of information and confidentiality**. The contract should spell out the service provider's obligation to keep private information private, 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.

- **Notification of cybersecurity breaches**. The contract should identify how quickly the plan sponsor would be notified of any cyber incident or data breach. The foregoing information should also be reflected in a business associate agreement. In addition, the contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.

- **Compliance with records retention and destruction, privacy, and information security laws**. The contract should specify the service provider's obligations to meet 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.

- **Insurance**. The contract should reflect the service provider's insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and fidelity bond/blanket crime coverage. The plan fiduciary should understand the terms and limits of any coverage before relying upon it as protection from loss.

Once engaged, the service provider's cybersecurity should be audited and validated.

Cybersecurity Program Best Practices

Consistent with an ERISA fiduciary's duties to act prudently and in the best interest of the plan participants and beneficiaries, the fiduciary has an obligation to protect plan assets and data from access by cybercriminals and have processes in plan to mitigate cybersecurity breaches. The DOL has 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 to be considered for engagement. Pursuant to the guidance, plan service providers should:

- Have a formal, well-documented cybersecurity program that identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information.
- Conduct prudent annual risk assessments to identify, estimate, and prioritize information system risks.
- Have an independent auditor assess an organization's security controls and provide a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.
- Clearly define and assign information security roles and responsibilities, which should be managed at the senior executive level and executed by qualified personnel who establish and maintain the vision, strategy, and operation of the cybersecurity program.
- Have strong access control procedures to guarantee that users are properly identified and have the appropriate access to IT systems and data, mainly consisting of authentication and authorization.
- 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.
- Conduct periodic cybersecurity awareness training because employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat.
- Implement and manage a secure system development life cycle (SDLC) program to ensure that security assurance activities such as penetration testing, code review, and architecture analysis addressed.
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypt sensitive data, stored and in transit, which implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.
- Implement strong technical controls in accordance with best security practices. Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
- Appropriately respond to any past cybersecurity incidents. When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its

participants, including informing law enforcement and participants and fixing the problem that caused the breach.

Online Security Tips

Plan sponsors can assist participants in protecting confidential personal and plan asset information, and reduce the likelihood of fraud, by encouraging participants to routinely monitor online benefits accounts. Strong and unique passwords should be used in addition to multi-factor authentication.

Plan sponsors should also ensure that they maintain the most current contact information for participants in the event needed to immediately communicate any cybersecurity breach. Additionally, the plan sponsor should have a policy of advising participants to avoid the use of free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops pose security risks that may give criminals access to personal information.

Plan sponsors should have processes in place to mitigate phishing attacks intended to trick participants into sharing passwords, account numbers, and sensitive information, and access to accounts. Plan sponsors are encouraged to implement and maintain trustworthy antivirus software installed and updated to protect workplace computers and mobile devices to protect against viruses and malware. Software should also be kept current with the latest patches and upgrades.

Last, the FBI and the Department of Homeland Security have set up the following valuable sites for reporting cybersecurity incidents that plan sponsors are encouraged to utilize:

https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

https://www.cisa.gov/reporting-cyber-incidents