Verrill

DOL Cybersecurity Guidance

by Lisa S. Boehm on June 23, 2021

This post provides a high-level summary of the Department of Labor's cybersecurity guidance issued in April and identifies actions retirement plan sponsors and other plan fiduciaries should consider taking now in light of the guidance and the fact that the DOL has started sending information requests under an audit initiative concentrating on cybersecurity practices.

The cybersecurity guidance addresses three principal areas: (1) online security tips for retirement plan participants and beneficiaries (available here), (2) tips for plan sponsors and other plan fiduciaries to prudently select and monitor retirement plan recordkeepers and other service providers (available here), and (3) best practices for retirement plan recordkeepers, and for plan fiduciaries responsible for selecting and monitoring retirement plan recordkeepers and service providers, to manage cybersecurity risks (available here).

Online Security Tips for Participants and Beneficiaries. These tips are basic protections that participants and beneficiaries should take whenever personally identifiable information ("PII") is being transmitted or stored. The tips are intended to keep PII, and retirement plan accounts and benefits, safe, and they include using strong and unique passwords, periodically changing passwords (the DOL suggests every 120 days), using multi-factor authentication, ensuring all personal contact information is up to date, establishing and routinely monitoring online retirement accounts, and being wary of free Wi-Fi networks.

- Plan Fiduciary Action Item: As part of its on-going monitoring responsibilities, a retirement plan fiduciary should confirm with the plan recordkeeper that these basic protections are available to all plan participants and beneficiaries and document its inquiries regarding the availability of these features and the recordkeeper's responses.

Tips for Selecting and Monitoring Service Providers. These tips include a series of questions to ask a service provider about its information security standards, policies, practices and procedures and cybersecurity audit results; past security breaches, if any, and how the service provider responded; and any insurance policies it has that would provide coverage for losses caused by cybersecurity breaches and identity theft. The tips also include cybersecurity and information security-related provisions that should be included in the written agreement with a service provider and evaluating the service provider's track record in the industry, including review of public information regarding security incidents, litigation, and legal proceedings related to the services it provides.

- Plan Fiduciary Action Items: See *Best Practices for Recordkeepers and Plan Fiduciaries to Manage Cybersecurity Risk* below.

Best Practices for Recordkeepers and Plan Fiduciaries to Manage Cybersecurity Risk. The DOL guidance sets forth twelve best practices for use by recordkeepers and other service providers responsible for retirement plan-related IT systems and data, and for retirement plan fiduciaries making prudent decisions regarding the service providers they engage. These best practices can be grouped into three general categories.

The first category is establishment of a fundamentally sound cybersecurity program designed to identify and assess internal and external cybersecurity risks that may threaten the integrity, confidentiality, and availability of stored nonpublic information. A robust cybersecurity program consists of strong security policies, practices, procedures, and standards to protect the security of the IT infrastructure and data stored on the system ("security measures"). Examples of these security measures include encryption of PII and other sensitive data, both while in transit and in storage; strong access control procedures; re-occurring cybersecurity awareness training; security assurance activities such as penetration testing, code review and architecture analysis; and a business resiliency program that includes a business continuity plan, a disaster recovery plan and an incident response plan.

The second category is having a solid governance framework to implement and administer the cybersecurity program. This means the recordkeeper and other service providers should have a formal, written implementation plan in place, a senior level executive (*e.g.*, a Chief Information Security Officer) responsible for developing, managing, and updating the cybersecurity program and implementation plan, and an internal team of qualified cybersecurity personnel to execute the implementation plan.

The third category is on-going monitoring of the cybersecurity program. Recordkeepers and other service providers should conduct annual risk assessments and engage a reliable independent auditor to assess their security controls on an annual basis (*e.g.*, a service organization control report, known as a SOC 2 report). Service providers must continually monitor their cybersecurity program and continually update it as a result of the annual risk assessments and SOC 2 reports. There is no "set it and forget it" notion when it comes to a cybersecurity program because IT threats are constantly changing.

While the DOL's best practices may be intended primarily for recordkeepers, plan fiduciaries should also use them when evaluating other current and prospective service providers (*e.g.*, custodians, trustees, auditors, and actuaries).

- Plan Fiduciary Action Items: When selecting or monitoring a recordkeeper or other service provider, at a minimum plan fiduciaries should:

- Request and review the provider's security policies, practices, procedures, and standards and SOC 2 audit results, with assistance from an independent information security consultant as needed
- Request and review any insurance policies purchased by the provider to cover internal and external cybersecurity breaches and identify theft
- Review service provider agreements for provisions (1) permitting the plan sponsor or other applicable fiduciary to conduct an independent audit of the provider's cybersecurity program by an independent security specialist, (2) addressing whether the provider has the right to use participant data for purposes of offering other services unrelated to the retirement plan or to provide participant data to third parties, and (3) providing any cybersecurity guarantees or limitations on liability for cybersecurity breaches or identity theft
- Ask about any cybersecurity breaches and identity theft, including the provider's responses and any litigation
- Determine whether any third parties have access to participant data and for what purpose
- Ask about the provider's compliance with record retention and destruction laws
- Consider engaging a cybersecurity specialist to review the provider's responses and documentation provided and identify any deficiencies
- As with fees, periodically assess what other recordkeepers and service providers have in place for cybersecurity policies, practices, procedures, and standards and do some benchmarking against industry standards
- Document the review process, questions asked, and the service provider's responses – documentation is the best evidence of a prudent process

Additional Considerations for Plan Fiduciaries. It seems clear that in issuing its cybersecurity guidance, the DOL is setting minimum expectations for addressing cybersecurity risk in retirement plans. In light of the guidance, plan fiduciaries should also consider including a review of cybersecurity responsibilities in fiduciary training, periodically discussing cybersecurity industry trends in their meetings, requesting periodic updates from recordkeepers and other service providers on their cybersecurity programs, monitoring retirement plan cybersecurity procedures and practices internally within their organization, engaging a cybersecurity specialist to assist them in monitoring cybersecurity matters (both internal and external), purchasing insurance that may be available to protect the retirement plan, participants, and beneficiaries, in the event of a cybersecurity breach or identity theft, and educating participants and beneficiaries on actions they should take to protect their PII and retirement plan benefits.

Please contact a member of Verrill's Employee Benefits & Executive Compensation Group if you have questions about mitigating cybersecurity risk in retirement plans.

Lisa S. Boehm
Partner
T (207) 253 4904
email