GROOM LAW GROUP

www.groom.com

DOL Issues Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, and Plan Participants

PUBLISHED: April 16, 2021

On April 14, 2021, the U.S. Department of Labor ("DOL") issued a cybersecurity guidance package directed to plan sponsors; fiduciaries regulated under the Employee Retirement Income Security Act of 1974, as amended ("ERISA"); recordkeepers and other service providers; and participants and beneficiaries. This is DOL's first guidance directly addressing cybersecurity. In fact, the U.S. Government Accountability Office ("GAO") recently urged DOL to issue guidance identifying minimum expectations for mitigating cybersecurity risks. DOL's cybersecurity guidance package is presented in three separate documents:

1. Tips for Hiring a Service Provider with Strong Cybersecurity Practices;
2. Cybersecurity Program Best Practices; and
3. Online Security Tips.

The guidance is written as "tips" and "best practices." However, the guidance itself, particularly the Cybersecurity Program Best Practices document, does appear to attempt to establish minimum expectations that DOL may have more appropriately issued under a notice and comment process.

Notably, while some of the guidance package is framed in the context of retirement plans, the guidance appears to apply to all ERISA plans, including health and welfare plans, as the underlying fiduciary responsibilities and obligations are equally applicable in both contexts. Health plans that are subject to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), likely will need to review the DOL guidance on top of their HIPAA obligations to see if there are any additional gaps to fill.

If you have any questions, please do not hesitate to contact your regular Groom attorney or the authors listed below:

Jennifer Eller
jeller@groom.com
(202) 861-6604

Allison Itami
aitami@groom.com
(202) 861-0159

David Levine
dlevine@groom.com
(202) 861-5436

Christy Tinnes
ctinnes@groom.com
(202) 861-6603

Vivian Hunter Turner
vturner@groom.com
(202) 861-6324

Jeanne Klinefelter Wilson
jwilson@groom.com
(202) 861-6613

DOL's guidance is grounded in the premise that responsible plan fiduciaries have a duty to mitigate cybersecurity risk. DOL also recognizes that participants and beneficiaries have an important role in cybersecurity. In the future, in the context of a benefit loss sustained by a participant due to a cybersecurity breach, possibly this guidance could be used as a reference to allocate responsibility for that loss, either in DOL enforcement actions, settlement actions, or even by courts.

In this alert, we provide an overview of DOL's cybersecurity guidance, starting with a plan fiduciary's obligation to mitigate cybersecurity risk. Then we discuss the details of each of the DOL documents issued as part of the cybersecurity guidance package. Finally, we end with insights regarding how this guidance will affect sponsors, fiduciaries and providers.

I. Plan Fiduciaries Must Mitigate Cybersecurity Risk

DOL's cybersecurity guidance package states that responsible plan fiduciaries have a duty to mitigate a plan's cybersecurity risks. DOL made similar statements in the last twelve months in two other contexts. In the preamble to final regulation on Default Electronic Disclosure by Employee Pension Benefit Plans Under ERISA, published May 27, 2020 (the "Electronic Disclosure Final Rule"), DOL said that ERISA's fiduciary duties generally require plans to have secure systems in place to protect individuals' personal information. Accordingly, one condition to meeting the safe harbor established by the Electronic Disclosure Final rule is that a plan administrator (possibly in coordination with plan service providers), take measures reasonably calculated to protect the confidentiality of personal information. The preamble explained that this confidentiality obligation extends to both the security of, and the privacy of, participant information.

In February of 2021, GAO issued a report titled "Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans" (the "GAO Report"). In that report, GAO urged DOL to issue a statement that "cybersecurity for ERISA covered plans is a plan fiduciary responsibility." DOL's response, which was included in the report, however, stopped short of categorically stating that a fiduciary is responsible for fail-safe cybersecurity. Instead, DOL's response said that plan fiduciaries have a duty to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise. DOL's response to GAO also said that plan fiduciaries must include cybersecurity considerations in the selection process for service providers, including ensuring that electronic recordkeeping systems have reasonable controls and are maintained in a safe and accessible place with adequate records management practices.

This cybersecurity guidance package, issued after DOL's response to the GAO Report, shifts from DOL's previous principles-based approach to a much more prescriptive approach.

II. Plan Sponsor and Plan Fiduciary Guidance: Tips for Hiring a Service Provider with Strong Cybersecurity Practices

According to DOL, ERISA requires plan sponsors and fiduciaries to prudently select and monitor service providers with strong cybersecurity practices. DOL's tips for hiring service providers include due diligence items and contracting suggestions meant to apply plan sponsors of all sizes.

A. Due Diligence

DOL's tips for hiring and monitoring service providers suggest significant due diligence obligations. Plan sponsors should consider including DOL's suggested inquiries in any RFP or selection process for a service provider. Moreover, plan sponsors may want to take steps to evaluate existing service providers using DOL's inquiries. DOL's suggested due diligence steps include the following:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare that information to industry standards adopted by other service providers. According to DOL, plan fiduciaries should look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. DOL states that a plan fiduciary can have "much more confidence" in the service provider's systems and security practices if they are backed by annual audit reports verifying information security, system/data availability, processing integrity, and data confidentiality.
2. Ask how the service provider validates its cybersecurity practices, and what levels of security standards are in place.
3. Evaluate the service provider's "track record" in the industry, including public information about information security incidents, other litigation, and legal proceedings related to the vendor's services.
4. Ask whether the service provider has experienced past security data breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses covered 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).

B. Contracting

DOL's tips on contracting with a service provider state that plan fiduciaries should "beware [of] contract provisions that limit the service provider's responsibility for IT security breaches" and should "look for" or "try to include" certain contract provisions. DOL's tips for contract provisions are outlined below. While DOL's tips in this particular document are not a checklist, there may be a concern that in the event a of cybersecurity breach, DOL may scrutinize contracts that limit a service

provider's IT security breach obligations and that do not include the recommended provisions. DOL's tips for contract provisions extend to including the following:

1. Information Security Reporting: Requiring the service provider to obtain a third-party audit annually to determine compliance with information security policies and procedures.
2. Clear Provisions on the Use and Sharing of Information and Confidentiality: Specifying and defining a service provider's obligations to maintain the confidentiality of private information; to prevent the use or disclosure of confidential information without written permission; and to employ a strong standard of care to protect against unauthorized access, loss, disclosure, modification, or misuse of confidential information.
3. Notification of Cybersecurity Breaches: Specifying the service provider's obligations to meet all applicable laws (federal, state, and local) applicable to the privacy, confidentiality, or security of participants' personal information.
4. Insurance: Requiring insurance coverage such as professional liability, errors and omissions liability, cyber liability and privacy breach, and/or fidelity bond/blanket crime coverage. DOL states that a plan fiduciary should understand the terms and limits of any such coverage.

III. Recordkeepers and Other Service Providers: Cybersecurity Program Best Practices

DOL's Cybersecurity Program Best Practices are addressed to recordkeepers and other service providers. Each of the 12-point best practices listed below is accompanied by a prescriptive set of conditions within the DOL document. The practices are:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. 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.
7. Conduct annual cybersecurity awareness training.
8. Implement and manage a secure system development life cycle ("SDLC") program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

IV. Online Security Tips

DOL's cybersecurity guidance package includes a tip sheet for participants. The tip sheet itself is evidence of DOL's recognition that participants may unwittingly put their own retirement savings, or even a retirement plan, at risk if a participant does not follow safe practices.

DOL's Online Security Tips sheet advises participants to register, set up, and routinely monitor their online retirement accounts because failing to establish an account could enable online cybercriminals to assume a participant's identity. The Online Security Tips includes a discussion of strong and unique passwords, multifactor authentication, the importance of current contact information, deleting unused accounts, avoiding free Wi-Fi, not falling prey to phishing attacks, and antivirus software and security updates. Finally, the Online Security Tips sheet includes contact information to report identity theft and security incidents.

V. Insights

While largely based upon industry practice and mainly consistent with fiduciary practice for many, the DOL's cybersecurity package and its website release may foreshadow future enforcement initiatives. The document directed to service providers references what DOL might "expect to see" during a review of cybersecurity practices. By moving away from DOL's principles based approach adopted in the Electronic Disclosure Rule, the package ignores a service provider's expertise and unique vantage point for efficiently tailoring cybersecurity to its own situation.

The guidance also leaves a number of unanswered questions, particularly for health plans. Health plans and business associates commonly turn to guidance issued by the National Institute for Standards and Technology ("NIST"), which provides a cybersecurity framework with specific workflow and standards for implementing security controls, when implementing the HIPAA Security Rule. The NIST guidance addresses a number of points outlined in the DOL guidance, such as audit requirements, training, and authentication requirements. It is not clear whether the Department of Health and Human Services Office of Civil Rights ("HHS"), which enforces HIPAA, will consider these DOL "best practices" to supplement the existing requirements outlined in the HIPAA Security Rule. Will HHS give any weight to DOL's guidelines?

In the event of a loss from a cybersecurity breach, possibly this package may serve as a standard to determining whether a plan fiduciary acted in a prudent manner. Fortunately, DOL's guidance recognizes that plan participants play an important role in the security of their own savings.

Plan fiduciaries are advised to review their service provider hiring practices and contracts with their service providers in light of DOL's tips and best practices. Finally, plan fiduciaries should consider distributing DOL's online security tips to plan participants and keeping a record of that distribution.

Plan service providers may want to consider reviewing their approach to cybersecurity in light of the "Best Practices" guidance from the Department and documenting why the provider believes that its

approach is appropriate under the circumstances. Providers may also want to ensure that service contracts unambiguously address the provider's responsibilities with respect to cybersecurity and leave no doubt that the parties do not intend for the provider to act as a fiduciary with respect to plan data.