The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 33475

April 21, 2021

DOL Issues Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-keepers, and Plan Participants

[33475]

April 16, 2021 TO: ICI Members
Bank, Trust and Retirement Advisory Committee
Broker/Dealer Advisory Committee
Operations Committee
Pension Committee
Pension Operations Advisory Committee
Small Funds Committee
Transfer Agent Advisory Committee SUBJECTS: Pension RE: DOL Issues Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-keepers, and Plan Participants

The Department of Labor (DOL) recently issued a guidance package in the form of "tips" and "best practices" on cybersecurity relating to retirement plans covered by ERISA.[1] While the GAO and the ERISA Advisory Council have examined this issue in recent years, this is the first time that DOL has issued guidance on cybersecurity.[2] The guidance includes three items:

- Tips for Hiring a Service Provider: Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.[3]
- Cybersecurity Program Best Practices: Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.[4]
- Online Security Tips: Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.[5]

As noted above, the guidance is presented in the form of tips and best practices and does not explicitly set minimum standards—although the best practices may come to be viewed as minimum standards. DOL does not discuss legal issues—such as who is responsible for losses that result from a cyber attack—other than to note that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."[6]

Tips for Hiring a Service Provider

DOL provides six tips that plan sponsors can use to select service providers that follow strong cybersecurity practices. The sixth tip is that the plan sponsor should make sure that

the contract with the service provider ensures ongoing compliance with cybersecurity and information security standards and should beware of provisions that limit the service provider's responsibility for security breaches. DOL suggests the following contract terms:

- Information Security Reporting. The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.
- 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. 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 plan sponsor may want to require insurance coverage such as professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and/or fidelity bond/blanket crime coverage. Be sure to understand the terms and limits of any coverage before relying upon it as protection from loss.

In addition to the suggested contract terms, DOL provides the following five tips:

- 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.
- Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented.
- 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.

Cybersecurity Program Best Practices

DOL describes the following twelve best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data:

- Have a formal, well documented cybersecurity program.
- Conduct prudent annual risk assessments.
- Have a reliable annual third-party audit of security controls.
- Clearly define and assign information security roles and responsibilities.
- 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.
- Conduct periodic cybersecurity awareness training.
- Implement and manage a secure system development life cycle (SDLC) program.
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypt sensitive data, stored and in transit.
- Implement strong technical controls in accordance with best security practices.
- Appropriately respond to any past cybersecurity incidents.

Tips for Plan Participants and Beneficiaries

DOL's online security tips for plan participants include the following:

- Register, set up, and routinely monitor your online account.
- Use strong and unique passwords.
- Use multi-factor authentication.
- Keep personal contact information current.
- Close or delete unused accounts.
- Be wary of free wi-fi.
- Beware of phishing attacks.
- Use antivirus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.

Shannon Salinas
Associate General Counsel - Retirement Policy

endnotes

[1] DOL's press release regarding the new guidance, issued April 14, 2021, is available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414. In the press release, DOL notes the connection between this guidance and its rules on electronic delivery. "The guidance announced today complements EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries. These include provisions on ensuring that electronic recordkeeping systems have reasonable controls, adequate records management practices are in place, and that electronic disclosure systems include measures calculated to protect Personally Identifiable Information." For a summary of DOL's most recent rule on electronic delivery, see ICI Memorandum No. 32478, dated May 21, 2020, available at https://www.ici.org/my_ici/memorandum/memo32478.

[2] The GAO recently released a new report, "Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans," Feb 11, 2021, available at https://www.gao.gov/products/gao-21-25. In 2016, the ERISA Advisory Report studied the topic "Cybersecurity Considerations for Benefit Plans," and its report is available at https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

[3] Tips for Hiring a Service Provider is available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf.

[4] Cybersecurity Program Best Practices is available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

[5] Online Security Tips is available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

[6] See page 1 of Cybersecurity Program Best Practices. In a letter from DOL included at page 34 of the recent GAO report, DOL states that "plan fiduciaries must act prudently and solely in the interests of plan participants and beneficiaries, as set forth in ERISA section 404. In the Department's view, these duties require plan fiduciaries to take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise. That legal framework obligates fiduciaries, among other things, to include cybersecurity considerations in the selection process for service providers."
