Chapman and Cutler LLP

Chapman Client Alert

April 16, 2021 Current Issues Relevant to Our Clients

U.S. Department of Labor Announces Cybersecurity Guidance for Plan Sponsors, Fiduciaries and Participants

On April 14, 2021, the U.S. Department of Labor (the *"DOL"*) announced guidance for plan sponsors, plan fiduciaries, record keepers, and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of participants. The guidance comes in three forms: (1) Tips for Hiring a Service Provider, (2) Cybersecurity Program Best Practices, and (3) Online Security Tips. Although there is no new law or regulation, it is the first time the DOL has issued cybersecurity guidance, which may provide a blueprint for required conduct by plan sponsors and fiduciaries in fulfilling their respective obligations to a plan and its participants.

Tips for Hiring a Service Provider

The DOL presented the following items for plan sponsors and fiduciaries to evaluate when conducting diligence in selecting plan service providers and monitoring the performance of the providers:

1. 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.

2. Ask the service provider how it validates its practices, what levels of security standards it has met and implemented, and whether there are contract provisions that give the fiduciary the right to review audit results demonstrating compliance with the standards.

3. 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 services.

4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

5. Determine 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 participant's account).

6. Ensure that the contract with the service provider requires ongoing compliance with cybersecurity and information security standards, and beware of contract provisions that limit the service provider's responsibility for security breaches. The DOL suggested additional contract provisions that could enhance compliance, such as (a) information security reporting, (b) clear provisions on the use and sharing of information, (c) notification of cybersecurity breaches, (d) compliance with records retention and destruction regulations, and (e) requiring insurance coverage.

Documenting the responses to these items as evidence that a plan sponsor or fiduciary followed the guidance provided by the DOL and conducted a thorough investigation of the service provider will go a long way in demonstrating that fiduciary duties to the plan and participants have been met in the event something goes wrong at the service provider level. As in most contract negotiations, the ability to extract favorable contract provisions as suggested by the DOL will depend upon the leverage afforded the sponsor or fiduciary based on the size of the plan, the reputation and quality of service of the provider, and the terms offered by comparable service providers in light of the new guidance.

Cybersecurity Program Best Practices

The DOL admitted that ERISA-covered plans may be tempting targets for criminals and, as a result, stated that responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks. The following best practices were presented for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on retaining service providers. The best practices include that the service provider:

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 periodic cybersecurity awareness training;
8. Implement and manage a secure system development life cycle (*"SDLC"*) program;
9. Have an effective business resiliency program that addresses business continuity, disaster recovery, and incident response;
10. Encrypt sensitive data, both when stored and when in transit;
11. Implement strong technical controls in accordance with best security practices; and
12. Appropriately respond to any past cybersecurity incidents.

Specific details for each suggested best practice, including the DOL's suggested elements of a "sound cybersecurity program" which identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information, can be found here: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

Online Security Tips

As part of the guidance, the DOL also provided tips for plan participants in order to reduce the risk of fraud and loss to a retirement account by:

- Registering, setting up, and routinely monitoring the participant's online account;
- Using strong and unique passwords;
- Using multifactor authentication;
- Keeping personal contact information current;
- Closing or deleting unused accounts;
- Being wary of free Wi-Fi;
- Being wary of phishing attacks;
- Using antivirus software and keeping apps and software current; and
- Knowing how to report identity theft and cybersecurity incidents.

Although these tips are familiar to people in the financial industry, due to varying sophistication levels among plan participants, plan fiduciaries would be well served to provide a copy of the DOL's Online Security Tips to new clients or plan participants to alert them of the possibility of cyberattack and to provide the participant with tools to protect retirement savings that will augment the fiduciary's best practices relating to service provider selection. If a sponsor or fiduciary does not have its own document to provide clients, the Online Security Tips can be found here: https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.

For More Information

If you would like to discuss any topic covered in this Client Alert, please contact a member of the Investment Management group, or visit us online at chapman.com.

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®