Bolton Alert

April 2021

On April 14, 2021, the Department of Labor ("DOL") issued several pieces of guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity. This guidance encourages fiduciaries to consider cybersecurity issues when selecting and monitoring plan service providers such as recordkeepers, custodians, and third-party administrators. Fiduciaries have a responsibility to safeguard plan assets and participant data and the DOL's new guidance provides a framework for ensuring that controls are in place to avoid financial losses to plans that may result from a cybersecurity breach.

The Department of Labor has issued guidance on the following three distinct areas:

Tips for Hiring a Service Provider With Strong Cybersecurity Practices

The first piece of DOL guidance, Tips for Hiring Service Providers, outlines six factors for plan sponsors to consider when selecting retirement plan service 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, and what levels of security standards it has met and implemented.
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's services.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches.
6. When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service providers' responsibility for IT security breaches.

Cybersecurity Program Best Practices

The second piece of DOL guidance, Cybersecurity Best Practices, is focused on recordkeepers and other service providers responsible for plan-related IT systems. The DOL also makes the point that plan fiduciaries should be aware of these best practices to enable them to make prudent decisions when hiring a service provider. It is the most detailed of the three pieces of guidance which identifies the following 12 best practices that plan service providers "should" implement to mitigate exposure to cybersecurity risks.

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 addressing business continuity, disaster recovery,

and incident response
10. Encrypt sensitive data, stored in a transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

Online Security Tips

The third piece of DOL guidance, Online Security Tips, provides nine recommended security tips for plan participants and beneficiaries to keep their online information and account safe. The following basic rules are aimed at reducing the risk of fraud and loss:

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

Many plan service providers are already following the best practices recommended in the DOL's guidance. However, sound fiduciary practices are rooted in process and documentation of those processes. As such, Plan Sponsors should discuss the DOL guidance with their plan service providers and request documentation as evidence of their due diligence.

For more information, please contact our Senior Consultants, Mike Beczkowski, Alton Fryer, or Chris Bolton.