Department of Labor Cybersecurity Guidance

May 3, 2021

On April 14, 2021, the Department of Labor ("DOL") issued guidance for plan sponsors and recordkeepers on best practices for maintaining cybersecurity, as well as online security tips for plan participants and beneficiaries. The guidance is not legally binding, but is helpful in understanding the DOL's views regarding the role of plan fiduciaries and providers in maintaining cybersecurity.

Cybersecurity Program Best Practices

The DOL guidance identifies 12 suggested best practice protocols for use by recordkeepers and other service providers, and for plan fiduciaries to consider when choosing an entity to provide plan-related IT systems and data services to an employee benefit plan. The DOL recommends that service providers:

- 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 where it is stored and while in transit;
- Implement strong technical controls in accordance with best security practices; and
- Appropriately respond to any past cybersecurity incidents.

The guidance provides the above list both for service providers to use, and as a guide to plan fiduciaries when hiring a new service provider. Although not legally required, plans may want to confirm and document that existing service providers are in compliance or are taking steps to comply with the best practices. Also, although the guidance does not directly address the responsibilities of plan fiduciaries in safeguarding the plan's own data, it provides a helpful roadmap for plans to assess their own preparedness for a cyber incident.

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

The DOL encourages plan sponsors to select service providers with strong cybersecurity practices and then monitor their activities, consistent with their fiduciary duties under ERISA. The guidance encourages sponsors to:

- Ask the service provider about its information security standards, practices and policies and audit results, and compare them to industry standards;
- Ask how the provider validates its practices and what levels of security standards it has met and implemented;
- Evaluate its track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to the vendor's services;
- Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded;
- Confirm the service provider has insurance that covers losses caused by cybersecurity and identity theft breaches; and
- Include in contracts requirements for ongoing compliance with cybersecurity and information security standards and avoid contract provisions that limit the service provider's responsibility for IT security breaches.

In addition, the DOL recommends that plan sponsors include certain terms in provider contracts to enhance cybersecurity, such as those regarding information security reporting, confidentiality and the use and sharing of information, notification of cybersecurity breaches, compliance with records retention and destruction, privacy and information security laws, and insurance. Going forward, the DOL may look for these terms in provider contracts in the course of a plan audit.

The guidance does not address cyber liability insurance coverage for plans and plan sponsors. However, given the DOL's focus on cybersecurity, plans may wish to review whether their current cyber insurance covers losses related to breaches of electronic data and other cyber issues.

Online Security Tips for Participants and Beneficiaries

The DOL guidance includes tips for plan participants and beneficiaries aimed at reducing the risk of fraud and to protect their personal, financial and other information when they are using the internet to check their retirement accounts. These tips include:

- Using multi-factor authentication;
- Being wary of free Wi-Fi;
- Keeping personal contact information on the account current; and
- Closing or deleting unused accounts.

Please contact Slevin & Hart if you have questions about this guidance.

Attorneys

Zachary R. Gaines

Timothy K. Eicher