SpencerFane®

DOL Issues Cybersecurity Guidance

On April 14, 2021, the Department of Labor's Employee Benefits Security Administration ("EBSA") issued cybersecurity guidance for retirement plan fiduciaries and service providers, as well as plan participants. The guidance supplements the EBSA's electronic records and disclosures regulations and complements previous guidance issued by other agencies.

In the guidance, the EBSA states that ERISA fiduciaries are required to take appropriate steps to mitigate internal and external cybersecurity threats to plan participants and retirement plan assets. To assist fiduciaries and service providers in fulfilling this obligation, the EBSA issued two documents that describe cybersecurity best practices – Cybersecurity Program Best Practices and Tips for Hiring a Service Provider. The EBSA also issued some basic rules – Online Security Tips – to help participants reduce the risk of fraud and loss to their retirement accounts.

Cybersecurity Program Best Practices

To mitigate cybersecurity risks to retirement plans and their participants, the EBSA developed a set of best practices for retirement plan service providers and the plan fiduciaries selecting such providers. These practices include:

- **A formal, well documented cybersecurity program**: An organization's cybersecurity program should be designed to protect its IT infrastructure and information systems, as well as the data on such systems. The program should define and assign roles and responsibilities, and consist of procedures and standards to identify and respond to cybersecurity risks and events. In addition, the program should require (at least) annual cybersecurity awareness training.

- **Annual risk assessments**: Organizations should establish criteria for evaluating, assessing, and responding to cybersecurity risks as part of their risk assessments. In addition, the assessment process should be responsive to ever-changing technology and facilitate the revision of controls, as needed. Further, an organization storing data with a third-party service provider (such as a recordkeeper or custodian) should require a risk assessment of the provider, define minimum cybersecurity practices for the provider, and periodically assess the provider in connection with its continued service engagement.
- **Annual third-party security controls audits**: An organization's security controls should be reviewed by an independent auditor. The review should be well documented and include reporting in connection with penetration testing, cybersecurity practices, and corrections of any system vulnerabilities.
- **Strong access control procedures and technical controls**: Organizations should keep their system hardware, software, and firmware up to date and should routinely back up the data on their systems. In addition, system access should be limited to authorized users and follow a need-to-access principle. Policies and procedures should monitor system activity and require multi-factor authentication (whenever possible). Access privileges should be reviewed (and updated, if needed) at least every three months to ensure accuracy.
- **Encryption of sensitive data**: Organizations should implement current, prudent system standards to protect nonpublic information and to preserve the confidentiality and integrity of system data.
- **Business resiliency programs**: An organization should maintain a business resiliency program that consists of a business continuity plan, a disaster recovery plan, and an incident response plan. The program should provide procedures for an organization to follow to recover, resume, and maintain business functions in the event of a business disruption, as well as procedures for responding to security incidents.

Tips For Hiring A Service Provider

As described above, an effective cybersecurity program includes assessing and monitoring the cybersecurity programs of third-party service providers. The EBSA views these activities as part of a fiduciary's responsibility under ERISA in connection with the selection and monitoring of plan service providers. In short, the fiduciaries

should use service providers that have strong cybersecurity programs. To that end, the EBSA issued hiring tips for business owners and fiduciaries (regardless of size) that include:

- Asking the service provider about its information security standards, practices, policies and audit results. This information should be compared to industry standards adopted by other financial institutions.
- Identifying the levels of security standards implemented and maintained by the service provider and how the service provider validates its cybersecurity practices.
- Evaluating and investigating the service provider's experience with past security incidents and litigation, as well as how the service provider responded in these situations.
- Negotiating service agreements to include audit review rights, ongoing cybersecurity and information security compliance, service provider responsibility for security breaches with enhanced protections for participants, and appropriate insurance coverage for cybersecurity and identity theft breaches (whether caused by internal or external employees or contractors).

Online Security Tips

The EBSA also provided educational material for participants. While service providers and fiduciaries may find this information helpful, the tips are designed to provide plan participants with practices (and reminders) to mitigate fraud and loss in connection with their retirement accounts. Service providers and plan fiduciaries should consider furthering this effort by notifying participants of the information and how it can be accessed.

While the retirement plan industry is familiar with cybersecurity threats and attacks, plan fiduciaries and service providers may be uncertain about how to mitigate the associated risk. The EBSA's guidance provides long-awaited details to assist fiduciaries and service providers in their efforts to protect retirement plan participants and assets through the design and evaluation of strong cybersecurity programs and protocols. Plan fiduciaries and service providers should carefully review the EBSA's guidance to assess whether they are meeting their ERISA and business obligations with respect to cybersecurity.

This blog was drafted by Beth Miller, an attorney in the Spencer Fane Overland Park, Kansas office. For more information, visit www.spencerfane.com.