Schulte Roth&Zabel

Alert

DOL Issues First Cybersecurity Guidance for Plan Sponsors

May 17, 2021

On April 14, 2021, the U.S. Department of Labor ("DOL"), through its Employee Benefits Security Administration ("EBSA") issued its first set of guidance on cybersecurity for plan sponsors, plan fiduciaries, recordkeepers and plan participants. Given the increase in cybersecurity attacks against pension plans, and the potential vulnerability of approximately $9.3 trillion in benefit plan assets (per DOL estimation), EBSA's guidance on cybersecurity has been eagerly awaited and long overdue. In fact, in February 2021, the U.S. Government Accountability Office called upon the DOL to issue minimum cybersecurity standards.

EBSA's guidance is intended to complement the DOL's May 2020 regulations on electronic records and disclosures. While the 2020 regulations allow pension plans to transmit select plan documents electronically, such delivery created an increased risk of cybersecurity attacks. Though ERISA already requires plan sponsors to adhere to a high fiduciary standard to protect participants' and beneficiaries' benefits, EBSA's guidance represents a vital step towards helping plan sponsors, fiduciaries, recordkeepers and plan participants safeguard pension benefits and personal information. It also signals what the DOL will look for when auditing plans and service providers. Plan sponsors, fiduciaries and recordkeepers should therefore carefully review the guidance and heed EBSA's recommendations, including the action items we detail in this *Alert*, to ensure their cybersecurity programs meet EBSA's best practice standards.

In lieu of a set of FAQs or a formal regulation, the EBSA's guidance is made up of three "tip sheets," two of which are geared towards plan sponsors, fiduciaries and recordkeepers ("Tips for Hiring a Service Provider" and "Cybersecurity Program Best Practices"), and one of which is geared toward retirement plan participants and beneficiaries ("Online Security Tips").

While the guidance refers only to pension plans and benefits information, it serves as a helpful reference point for ERISA-covered welfare plans as well, to the extent such plans have not already put compliance programs in place that meet the requirements necessitated by HIPAA and/or other state and/or federal data security laws.

Tips for Pension Plan Sponsors, Fiduciaries and Recordkeepers

Cybersecurity Best Practices

For pension plan sponsors, fiduciaries and recordkeepers, EBSA provides guidance on cybersecurity best practices in 12 focus areas. In summary, EBSA recommends:

1. Having a formal, well-documented cybersecurity program that details security policies, procedures, guidelines and standards to protect the integrity and security of the information;

2. Conducting annual risk assessments that identify, estimate and prioritize information system risks;
3. Having a reliable annual third-party audit of security controls to provide an unbiased report of existing risks, vulnerabilities and weaknesses;
4. Clearly defining and assigning information security roles and responsibilities within the organization, and ensuring that there is someone on staff who is qualified to fulfill the role of an information security officer;
5. Having strong access control procedures to verify the identity of users, limit access to the specific information users require, and regularly review access privileges;
6. Ensuring that assets or data, if any, stored in the cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments;
7. Conducting periodic cybersecurity awareness training;
8. Implementing and managing a secure system development life cycle program ("SDLC") that integrates penetration testing, code review and architecture analysis;
9. Having an effective business resiliency program addressing business continuity, disaster recovery and incident response in the event of a breach to ensure that business operations are not interrupted and information remains safeguarded;
10. Encrypting sensitive data (both stored internally or externally and at rest or in transit) by using encryption keys, message authentication and hashing;
11. Implementing strong technical controls in accordance with best security practices, such as regularly updating hardware, software and firmware, utilizing vendor-supported firewalls and intrusion detection, implementing network segregation and conducting routine patch management; and
12. Appropriately responding to any past cybersecurity incidents, including, but not limited to, notifying the affected participant base and law enforcement (if applicable), and taking steps to mitigate the likelihood of a reoccurrence.

Tips for Hiring a Service Provider

When hiring and monitoring a service provider, EBSA recommends that plan sponsors, fiduciaries and recordkeepers inquire about potential service providers' cybersecurity programs and how such programs are maintained. Plan sponsors, fiduciaries and recordkeepers should compare potential service providers' cybersecurity programs to the industry standards adopted by other financial institutions, and should evaluate potential service providers' track records in the industry by reviewing public information about data security incidents and litigation. They should also ask potential service providers about whether they have experienced any cybersecurity incidents and how such incidents were handled, as well as whether the potential service provider has an insurance policy in place that would cover losses caused by cybersecurity breaches (including losses caused by internal and external threats). Plan sponsors, fiduciaries and recordkeepers should review service provider contracts to ensure that the contracts require the service providers to comply, on an ongoing basis, with cybersecurity and information security standards (and avoid contract provisions that limit service providers' responsibility for cybersecurity and information technology breaches). Finally, they should pay particular attention to contract terms relating to confidentiality, the use and sharing of information,

notice by the vendor of cybersecurity risk assessments and audit reports, cybersecurity breaches and records retention and destruction.

Tips for Plan Participants and Beneficiaries

For plan participants and beneficiaries who have access to their retirement benefit information online, EBSA recommends:

1. Registering, setting up and routinely monitoring retirement accounts to ensure no unauthorized changes have been made;
2. Using multi-factor authentication (such as a one-time code that is sent before logging in) and a strong and unique password, which should be changed relatively frequently;
3. Keeping personal information, such as cell phone numbers and email addresses, current, and closing or deleting unused accounts;
4. Avoiding free Wi-Fi and other unsecured internet access;
5. Being aware of phishing attacks and reporting any suspicious email before opening it;
6. Using antivirus software and running the most recent version of apps; and
7. Being familiar with resources on how to report identity theft and cybersecurity incidents.

Action Items

To comply with EBSA's guidance, plan sponsors, fiduciaries and recordkeepers should:

- Consider conducting an internal audit to get a sense of existing cybersecurity programs and potential areas of weakness;
- Develop written policies and procedures to ensure cybersecurity programs are clear and are kept up-to-date;
- Clearly define and assign information security roles and responsibilities, and have someone on staff who is qualified to fulfill the role of an information security officer;
- Train staff on how to spot potential cyber-attacks, such as phishing, and employ cybersecurity best practices;
- Review service provider contracts to ensure appropriate contractual protections, such as requirements to conduct annual audits and to make prompt notice of any security breaches;
- Conduct cyber due diligence on service providers, both at the time of engagement and periodically thereafter;
- Respond timely to any cybersecurity incidents;
- Confirm current business liability insurance coverage includes cybersecurity protection or obtain specific cybersecurity insurance coverage protection; and
- Consider preparing a participant communication that details EBSA's recommendations for cybersecurity safety and educates participants about their responsibility to participate in the process of mitigating cybersecurity risk.

Authored by Mark E. Brossman, Ronald E. Richman, Edward H. Sadtler, Susan E. Bernstein and Melissa J. Sandak.

If you have any questions concerning this *Alert*, or wish to update your policies, procedures and guidelines to reflect these measures, please contact your attorney at Schulte Roth & Zabel LLP or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com