MURTHA CULLINA

NEWS ALERT

EMPLOYEE BENEFITS

DOL Finally Issues Cybersecurity Guidance for Retirement Plans

By Melanie N. Aska and Erek M. Sharp | April 19, 2021

On April 14, 2021, the U.S. Department of Labor's (DOL's) Employee Benefits Security Administration (EBSA) finally issued first-ever guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity to protect the retirement benefits of America's workers under ERISA-subject private sector employer-sponsored retirement plans.

Background. The Employee Retirement Income Security Act of 1974 (ERISA) established minimum standards and requirements intended to protect plan participants and beneficiaries in private sector employer-sponsored retirement plans. However, since ERISA's enactment, plan sponsors and their service providers have increasingly relied on the internet and IT systems to execute tasks required to administer these retirement plans. In addition, plan sponsors often outsource retirement plan administration, including record keeping and other services, to third-party service providers, thus increasing the potential opportunities for cyber thieves and other bad actors to gain unauthorized access to accounts, participants' personally identifiable information (PII) and plan asset data. Protecting plan assets and participants' PII against cyber-attacks is a paramount issue for those involved with ensuring retirement security. (PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security Number, and other types of personal information that can be linked to an individual, such as medical, educational, financial and employment information.)

Much is at stake here. This country's private sector employer-sponsored retirement plans collectively hold trillions of dollars of assets for the benefit of millions of participants, and cybersecurity risks to those plans' assets and participants' PII is very real and growing. As of 2018, EBSA estimates that there were 106 million 401(k) and other defined contribution plan participants and 34 million defined benefit plan participants in private-sector plans collectively holding estimated assets of $9.3 trillion. In many cases, these funds are a participant's only savings for retirement, underscoring the importance of protecting these assets from cyber attacks.

DOL's First-Ever Cybersecurity Guidance. The DOL's first-ever public-facing cybersecurity guidance for retirement plans was posted to the DOL's webpage on April 14, 2021, and is available at https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity.

According to the accompanying DOL News Release (available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414), the DOL's cybersecurity guidance is intended to complement existing DOL regulations on electronic records and disclosures to plan participants and beneficiaries, which include provisions on ensuring that electronic recordkeeping systems have reasonable controls and adequate record management practices in place, and that electronic disclosure systems include measures calculated to protect participants' PII.

The DOL's cybersecurity guidance takes the following three forms:

- *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* (available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf), which is intended to help plan sponsors and fiduciaries prudently select service providers with strong cybersecurity practices and monitor their activities, as ERISA requires;

- *Cybersecurity Program Best Practices* (available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf), which is intended to assist plan fiduciaries and record keepers in their responsibilities to manage cybersecurity risks; and finally

- *Online Security Tips* (available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf), which offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

Focusing In on the Three Pieces of DOL Cybersecurity Guidance. The three pieces of DOL cybersecurity guidance are full of "tips" and "best practices", summarized below:

- *Tips for Hiring a Service Provider with Strong Cybersecurity Practices.* This piece of guidance offers six "tips" to help plan sponsors and fiduciaries meet their responsibilities under ERISA to prudently select and monitor retirement plan service providers to ensure that they use service providers that follow strong cybersecurity practices:

    1. Ask about the service provider's information security standards, practices and policies, and audit results, compare them to the industry standards adopted by other financial institutions, and look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity;

    2. Ask the service provider how it validates its practices and what levels of security standards it has met and implemented, and look for contract provisions that give the plan sponsor or fiduciary the right to review audit results demonstrating compliance with the standard;

    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 the 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 identify 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); and finally,

    6. When contracting with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards (and beware of contract provisions that limit the service provider's responsibility for IT security breaches), and also try to include terms in the contract that would enhance cybersecurity protection for the plan and its participants.

- *Cybersecurity Program Best Practices*. The second piece of DOL guidance offers the following twelve "best practices" for use by retirement plan record keepers and other plan service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire (the list below is just a summary, so for all the details, go to https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf). The guidance states that plan service providers should:

    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 and in transit;
    11. Implement strong technical controls in accordance with best security practices; and finally
    12. Appropriately respond to any past cybersecurity incidents.

- *Online Security Tips*. The final piece of DOL cybersecurity guidance offers plan participants and beneficiaries who check their retirement accounts online the following nine basic rules to reduce the risk of fraud and loss (the following list is just a summary, so for all the details, go to https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf):

    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; and finally
    9. Know how to report identify theft and cybersecurity incidents.

The DOL's Cybersecurity Guidance Is Long-Overdue. It has taken the DOL a very long time to issue cybersecurity guidance for ERISA-subject retirement plans. In 2011 and again in 2016, the Advisory Council on Employee Welfare and Pension Benefit Plans (the ERISA Advisory Council) released two reports to the DOL that focused on privacy and cybersecurity issues affecting employee benefit plans, but the DOL failed to act on either report. EBSA recently told the U.S. Government Accountability Office (GAO), Congress' "watchdog", that it had released the ERISA Advisory Council's two reports to the public through the EBSA's website, but had not taken or planned to take any action on the reports' recommendations.

In February 2021, the GAO itself issued a report to Congressional requestors, *Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans* (available at https://www.gao.gov/products/gao-21-25), which, after noting that substantial cybersecurity risk mitigation measures had already been put into place by both private sector industries and by certain U.S. federal agencies (other than the DOL), recommended that the DOL should:

- Formally state whether cybersecurity for private-sector employer sponsored defined contribution retirement plans is a plan fiduciary responsibility under ERISA; and

- Develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks that outline the specific requirements that should be taken by all entities involved in administering private sector employer-sponsored defined contribution retirement plans.

The DOL's April 14, 2021 cybersecurity guidance appears to be at least a first step toward following the GAO's recommendations. It remains to be seen, however, whether following the DOL's guidance would provide an effective defense for plan sponsors, plan fiduciaries and plan service providers that are sued by plan participants who have lost their retirement plan nest eggs to cyber thieves or other bad actors. Perhaps in time, the DOL will offer up additional guidance, meatier than "tips" and "best practices", setting forth clear standards and requirements that plan sponsors, plan fiduciaries and third-party service providers must meet to fulfill their respective ERISA duties owed to plan participants and beneficiaries.

If you have questions about the DOL's April 14, 2021 guidance on retirement plan cybersecurity or how that guidance might affect your business, please contact Melanie N. Aska, Counsel, at 617-457-4131 or maska@murthalaw.com or Erek M. Sharp, Partner, at 203-772-7772 or esharp@murthalaw.com.