EPSTEIN BECKER GREEN

Employee Benefits and Executive Compensation

CLIENT ALERT

EBSA Speaks: New Guidance for Mitigating Retirement Plan Cybersecurity Risk

By Michelle Capezza and Christopher Lech

April 2021

On April 14, 2021, the U.S. Department of Labor's ("DOL's") Employee Benefits Security Administration ("EBSA") issued its first cybersecurity best practices guidance for retirement plans. The guidance is set forth in three parts and emphasizes that plan sponsors and fiduciaries must take steps to mitigate cybersecurity risks as part of the fiduciary obligations imposed on them by the Employee Retirement Income Security Act of 1974 ("ERISA"). To assist plan sponsors and fiduciaries with their responsibilities to prudently select and monitor service providers, the guidance outlines considerations they can use to determine that service providers follow strong cybersecurity practices. EBSA views this guidance as a complement to its regulations on electronic records and disclosures to plan participants and beneficiaries (i.e., that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems follow measures that protect personally identifiable information).

Cybersecurity guidance has long been anticipated by the benefit plan community as a result of numerous informal discussions and programs with EBSA representatives regarding cybersecurity for benefit plans, ERISA Advisory Council reports on plan cybersecurity, security and safeguard actions taken by industry service providers, and emerging litigation. Both reported and unreported cybersecurity breaches, as well as incidences of fraudulent retirement plan distributions, have raised questions concerning the scope of ERISA fiduciary responsibility for the cybersecurity of plan participant information, plan asset data, and accounts. Recently, in its February 2021 report, the U.S. Government Accountability Office ("GAO") further urged the DOL to issue cybersecurity guidance, and recommended that the DOL formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks in defined contribution plans. The DOL agreed with GAO's second recommendation but did not state whether it agreed or disagreed with the first one.

With the advancements in technology (including technological tools that have emerged to aid in the administration and delivery of employee benefits), the novel cybersecurity risks that those advancements bring, and the trillions of dollars in employer-sponsored

retirement plan assets alone, there is ongoing concern for both (i) the security of the plan participant data that is collected, transmitted, processed, and stored for employee benefit plans and (ii) the security of the assets in participant accounts. The new guidance is a step forward as it provides best practices and approaches to mitigate cybersecurity risks and further validates steps that have already been adopted by plan fiduciaries and service providers.

The first piece of guidance issued by EBSA contains "Tips for Hiring a Service Provider with Strong Cybersecurity Practices." An overarching takeaway from these tips is that fiduciaries (i) must be prudent in selecting plan service providers, (ii) should review the service providers' cybersecurity practices when selecting them, and (iii) should develop ongoing monitoring practices. In this guidance, EBSA has outlined considerations for due diligence items, and service agreement provisions, to ensure *"ongoing compliance with cybersecurity and information security standards,"* and to establish contract terms for data breach notifications; compliance with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information; and insurance.

The second piece of guidance issued by EBSA is "Cybersecurity Program Best Practices," which states that *"[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."* This is the first formal pronouncement from EBSA that plan fiduciaries are at least obligated to ensure proper mitigation of cybersecurity risk. The guidance is carefully worded, but, by implication, it appears to impose upon plan fiduciaries the obligation to conduct proper due diligence to confirm service provider adherence to prudent cybersecurity practices and procedures to indicate that plan participants' information, data, and accounts will be safeguarded on an ongoing basis and appropriate controls are in place, and that responsible cybersecurity breach response procedures are followed. Among other best practices, this guidance provides that plan service providers should have formal, well-documented cybersecurity programs; "conduct *prudent annual* risk assessments"; obtain "reliable annual third party audits of security controls"; "conduct periodic cybersecurity awareness training"; and "implement and manage a secure system development life cycle (SDLC) program." Plan sponsors and fiduciaries should also determine how to evaluate their service providers based on these best practices.

The third piece of guidance issued by EBSA is directed towards employee benefit plan participants, containing "Online Security Tips," advising how participants can help reduce the risk of cybersecurity attacks and threats to their retirement accounts. Among these tips, EBSA advises plan participants to use strong passwords and multi-factor authentication, as well as how to be aware of possible phishing attacks that may expose their retirement accounts to cybersecurity breaches. Although directed at plan participants, plan fiduciaries should be cognizant of what tools, procedures, and possible educational trainings they can offer to their plan participants to aid in mitigating cybersecurity risks.

Considerations and Next Steps for Retirement Plans

At this stage, the guidance set forth by EBSA is a step forward in expressing its view on the respective responsibilities among plan sponsors, fiduciaries, service providers, and plan participants when it comes to cybersecurity and retirement plans. The concept that plan sponsors and fiduciaries have a responsibility to mitigate cybersecurity risk should serve as a call to action to revisit existing service provider relationships and request the necessary information to evaluate the state of their benefit plan cybersecurity practices and procedures, and to incorporate this type of review on a go-forward basis with new and existing service providers. Undoubtedly, litigation will evolve in this area as the scope of plan fiduciary responsibility is further shaped. New laws and regulations will also evolve in this area and will need to be addressed.

To that end, as we have advised, plan sponsors and fiduciaries should (i) establish strong procedures, protocols, policies, and other safeguards to protect participants' data and their retirement accounts, and (ii) develop a process for prudent selection and monitoring of their plan service providers to ensure that they also maintain and follow strong cybersecurity and breach response procedures. If cybersecurity breaches do occur, plan fiduciaries should have an established response plan with their service providers so that they are better equipped to swiftly respond and mitigate damages. In the event that litigation ensues, plan sponsors and fiduciaries will be better able to defend against potential fiduciary breach claims if they can demonstrate that they followed prudent policies and procedures to mitigate cybersecurity risks.

Many plan sponsors and fiduciaries, as well as plan service providers, have already developed such policies and procedures, cognizant of the risks in administering their retirement plans. These policies and procedures, service agreements, overall safeguards, protocols, and breach response procedures should be reviewed and updated, or established if not yet in place, to reflect the desired aspects of EBSA's cybersecurity best practices guidance, which will serve to protect the plan participants, and withstand scrutiny.

* * *

For more information about this Client Alert, please contact:

Michelle Capezza
New York
212-351-4774
mcapezza@ebglaw.com

Christopher Lech
New York
212-351-3736
clech@ebglaw.com

IRS Circular 230 Disclosure

We inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of: (i) avoiding any tax penalty, or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in locations throughout the United States and supporting domestic and multinational clients, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com.