“A Long Time Comin’”: The DOL issues Cybersecurity Guidance | Fiduciary Focus Series

May 12, 2021

Categories:

Blogs
Fiduciary Focus
Tax Law Defined™ Blog

Authors:

Sarah N. Lowe

On April 14, 2021, the U.S. Department of Labor (DOL) issued guidance on cybersecurity for employee benefit plans. The three-part guidance is directed at plan sponsors and fiduciaries, plan service providers, and plan participants themselves.

Background

Cybersecurity guidance from the DOL has been a long time coming. Dramatic changes in technology and its use in benefit plan administration have occurred since the passage of the Employee Retirement Income Security Act of 1974 (ERISA), which provides minimum standards for most private retirement and health care plans intended to protect plan participants. Current benefit plan administration involves a significant amount of information about a benefit plan’s participants, including personal identifiable information (PII) and protected health information. Increases in the outsourcing of benefit plan administration to recordkeepers and/or other third-party administrators mean that there are multiple IT systems interfacing with one another. The retirement plan landscape’s shift from defined benefit plans to individual account defined contribution plans has exacerbated these trends. The fact that participants can generally access their retirement or health plan account means that home computers are often interacting with the third-party service provider or employer’s systems. The bottom line is that modern benefit plan administration requires the regular movement of both information and assets between multiple parties, which increases the access points for data breaches and bad actors.

As the integration of technology in employee benefit plan administration has become practically ubiquitous, the risks of exposure or losses due to cyberattacks or data breaches have exponentially increased. PII is very valuable to cybercriminals

because it is generally permanently associated with an individual and therefore has a very long shelf life. The amount of money held in U.S. retirement plans also makes them a rich target for hackers and other bad actors. With little statutory guidance other than in the health plan area, plan sponsors and fiduciaries have grappled with what their benefit plan duties are relative to cybersecurity. And, as the cybersecurity risks have increased, more recent litigation has targeted fiduciaries for breaching their fiduciary duties relative to cybersecurity.

Both in 2011[1] and in 2016, [2] the ERISA Advisory Councils have issued reports recommending that the DOL issue some form of cybersecurity guidance. In February 2021, the Government Accountability Office (GAO) issued the report, "Defined Contribution Plans: *Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans*" (emphasis added). The GAO report noted that no DOL guidance on cybersecurity existed and recommended that the DOL formally state whether mitigating cybersecurity risks are a plan fiduciary responsibility and provide guidance that identifies the minimum expectations for addressing cybersecurity risks.

Current Guidance

The DOL's three pieces of guidance only scratch the surface in providing helpful guidance for plan sponsors, fiduciaries, and service providers, but they should nevertheless be considered in implementing cybersecurity strategies in the administration of benefit plans.

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

This piece of the guidance sets forth steps and actions that plan sponsors and fiduciaries should undertake to prudently assess a third-party service provider's cybersecurity program and practices in compliance with ERISA. While directed towards retirement and 401(k) services providers, the principles would be generally applicable to any service provider. Though the guidance is geared toward the diligence necessary for a prudent hiring decision, it likewise sets forth a roadmap for prudent monitoring. The required

diligence includes recommended questions and action steps:

- What are the service provider's information security standards, practices and policies, and audit results?
    - *Compare these responses to industry standards adopted by other financial institutions. Look for providers who follow a recognized standard for information security, and obtain annual audits by third-party auditors to review and validate cybersecurity.*
- How does the service provider validate its practices? What levels of security standards does the service provider implement?
    - *Negotiate for the right to review audit results of the service provider's cybersecurity program. Even with an existing service provider, given the DOL's focus, consider requesting to see this audit and documenting your review of the same.*
- Has the service provider experienced past security breaches? If so, what happened, and how was the issue remediated?
    - *Perform diligence regarding the service provider's track record in the industry, including internet and litigation searches regarding security incidents, litigation, or other legal proceedings (e.g., investigations and consider how past security incidents were resolved, such as through cooperation with the plan sponsor or through litigation).*
- Does the service provider carry any insurance policies that would cover losses caused by cybersecurity and identity theft breaches and, if so, what is the scope of that insurance?

If, after considering the above questions in connection with a hiring decision, the plan sponsor or fiduciary decides to utilize a service provider in the administrator of a benefit plan, the DOL suggests a few contractual provisions that the plan sponsor or fiduciary should ensure that the contract contains. A few of those provisions are:

- Ongoing compliance with cybersecurity and information security industry standards—including DOL Cybersecurity Program Best Practices (discussed below)—and with all

applicable federal, state and local records retention and destruction, privacy, and information security laws;

- Provisions curtailing the use and sharing of plan participant information the service provider obtains in the administration of the plan;
- Policies to follow in the event of a cybersecurity breach (*g.*, notification requirements, cooperation requirements, and allocation of responsibility for implementing solutions); and
- An annual independent, third-party audit requirement to determine adequacy of the service provider's practices.

Plan sponsors and fiduciaries should consider whether the contract should require insurance coverage specific to cybersecurity threats (*e.g.*, professional liability and errors and omissions liability insurance, cyber liability and privacy breach insurance, and fidelity bond/blanket crime coverage).

Given that the majority of plan sponsors and fiduciaries likely already have existing service providers that aid in the administration of their benefit plans, plan sponsors and fiduciaries may consider amending the applicable service agreement to include some or all of the provisions recommended above to the extent there is not sufficient contractual protection under the existing agreement.

Cybersecurity Program Best Practices for Service Providers

This piece of guidance provides advice to recordkeepers and service providers responsible for plan-related IT systems and data. To satisfy their cybersecurity responsibilities under ERISA, recordkeepers and service providers should:

- Have a documented cybersecurity program that protects the plan participants' information from unauthorized access and provides policies for quickly identifying, assessing, and dealing with internal and external cybersecurity risks;
- Conduct prudent annual risk assessments to keep pace with changing IT threats;

- Have an annual independent, third-party audit of security controls;
- Have a senior executive oversee the cybersecurity program and qualified personnel implement it;
- Have strong access control procedures to ensure users' identities (*g.*, access privileges, multi-factor authentication);
- 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 to help employees recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat;
- Implement and manage a secure system development life cycle program to ensure applications used in the administration of the plan are developed securely;
- Prepare a business resiliency program which includes business continuity, disaster recovery and incident response plans;
- Encrypt sensitive data in accordance with industry standards;
- Implement strong technical controls with best security practices (*e.g.*, hardware, software, and firmware used in plan administration backed-up and up to date); and
- Appropriately respond to any cybersecurity incidents by investigating the incident and informing the appropriate authorities, insurer, and plan contacts.

More detail about these cybersecurity program best practices is set forth in this piece of guidance.

Online Security Tips

This piece of guidance is directed towards plan participants. The fact that the DOL issued this guidance acknowledges that plan participants also have a role to play in keeping their own data and assets secure. To reduce the risk of fraud and loss in a participant's account, the DOL recommends that plan participants:

- Routinely monitor their online account;

- Use strong and unique passwords;
- Use multi-factor authentication;
- Keep personal contact information current;
- Close or delete unused accounts;
- Be wary of free Wi-Fi;
- Beware phishing attacks;
- Use antivirus software and keeps applications and software current; and
- Know how to report identity theft and cybersecurity incidents.

Most participants will read these rules and think they are obvious. Nevertheless, plan sponsors and fiduciaries should encourage plan participants to keep these recommendations in mind.

Guidance is Guidance…Not Law

The DOL's three pieces of guidance are a step in the right direction and may provide plan sponsors, fiduciaries, and recordkeepers some direction as to how to comply with their duties in this area. However, the reality remains that DOL guidance is just that—guidance. The guidance does not have the full force of law or regulation. Nevertheless, failing to adequately respond to this guidance could increase the potential liability of plan sponsors or fiduciaries in connection with plan data or other cybersecurity breaches.

Next Steps

Plan sponsors and fiduciaries should consider what actions they should take in light of this guidance, particularly as it relates to plan service providers.

For help applying the DOL's guidance to your plan or questions about whether your plan is sufficiently protecting the plan's participants, please contact Sarah Lowe, Edward Rivin, or another attorney in Frost Brown Todd's Employee Benefits & ERISA practice group.

*Check out related articles in Frost Brown Todd's **Fiduciary Focus Series**, which provides critical updates and practical guidance related to retirement plans. You can also **SIGN UP** to receive updates on employee benefits and ERISA sent directly to your inbox.*

---

[1] The 2011 Advisory Council report suggested that the DOL should clarify whether there is a fiduciary duty to protect PII and, if so, the scope of that duty. Additionally, the 2011 report recommended, among other things, that the DOL should develop educational materials to help plan sponsors and administrators address privacy and security issues in benefit plan administration.

[2] Expanding on the findings of the 2011 report on cybersecurity considerations for benefit plans, the 2016 Council issued a follow-up report that focused on information it thought "would be useful to plan sponsors, fiduciaries, and their service providers in evaluating and developing a cybersecurity program for their benefit plans." The Council asked the DOL to issue guidance assisting plan sponsors and fiduciaries on how to evaluate cybersecurity risks affecting their plans, the various security frameworks that should be used to protect participant's data, and how to pick the right service provider to aid in the administration of the benefit plan. The November 2016 report can be found here and can provide some additional advice to plan sponsors, fiduciaries, and service providers on steps that can be taken to establish a strong cybersecurity program.

FBT Gibbons