April 22, 2021

Department of Labor Releases Cybersecurity Guidance

Recent cyberattacks have gotten a lot of attention. Some of these hacks have created turmoil through a broad swath of the business community. But another widespread menace threatens our financial security. In fact, even as you read this, the global threat of cybercrime continues around the clock as criminals try to steal retirement plan assets.

A recent Government Accountability Office (GAO) report recommended that the Department of Labor (among other things) establish minimum expectations for addressing cybersecurity risks in retirement plans. According to recent estimates, IRAs and defined contribution plans alone hold well over $10 trillion in assets. And they are ripe for exploitation. On April 14, the DOL's Employee Benefits Security Administration (EBSA) issued—for the first time—guidance for plan sponsors, fiduciaries, recordkeepers, service providers, and plan participants on best practices for maintaining cybersecurity. This guidance comes in three pieces.

1) Tips for Hiring a Service Provider. This piece helps employers and other fiduciaries to choose service providers that maintain solid cybersecurity practices.
2) Cybersecurity Program Best Practices. This guidance outlines ways that service providers can best address cybersecurity risks.
3) Online Security Tips. This release gives account owners suggestions on reducing the risk to their savings.

While the links above bring you to the full text of the DOL's guidance, here are some of the highlights from each.

Tips for Hiring a Service Provider with Strong Cybersecurity

Business owners want to run their businesses. So they often hire third-party vendors to handle matters outside their core competencies. This is also true for administering a retirement plan. Employers regularly look to recordkeepers, third-party administrators, and other service providers to conduct a plan's day-to-day operations. These suggestions may help business owners and others to select and monitor those who provide plan services.

- Ask about security standards, audit results, and other practices and policies; look for service providers that use an outside auditor to review cybersecurity.
- Look for contract provisions that allow a review of audit results to verify whether providers comply with industry standards.
- Ask about past security breaches—and about the provider's response to any such breaches.
- Find out whether they have sufficient insurance coverage to cover losses caused by identity theft and other cybersecurity breaches (both internal and external).

- Make sure that the contract requires ongoing compliance with cybersecurity and information security standards—and use caution if the contract limits responsibility for IT security breaches.
- Try to include additional cybersecurity-enhancement terms in the contracts, such as
    - a requirement that the provider obtain an annual security audit;
    - clear provisions on using and sharing confidential information;
    - prompt notification of security breaches, and an investigation into the causes of any breaches;
    - assurance of compliance with all laws pertaining to privacy, confidentiality, or security of participants' personal information; and
    - adequate insurance coverage (including for errors and omissions, cyber liability, and data breach), which employers should understand to avoid surprises.

Cybersecurity Program Best Practices

This second EBSA piece points out that "responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks." Keep in mind that many service providers carefully avoid taking on an employer's fiduciary duties. This does not mean, however, that these providers are somehow abdicating their responsibilities. To the contrary, most service providers recognize that, in order to compete in today's retirement plan marketplace, they must adhere to the highest compliance standards. And employers—as fiduciaries—must select and monitor providers to make sure that these standards are met. So these EBSA best practices can help employers meet their own fiduciary duties by "making prudent decisions on the service providers they should hire." They can also help service providers see how their current practices measure up, and then take action to improve any deficiencies.

EBSA lists 12 practices that a plan's service provider should adhere to.

1) *A formal, well-documented cybersecurity program.* The organization should fully implement a program that identifies internal and external cybersecurity risks.
2) *Prudent annual risk assessments.* The organization should document the assessment's scope, methodology, and frequency.
3) *Reliable annual third-party audit of security controls.* An independent auditor should assess the organization's security program—including any documented corrections of weaknesses.
4) *Clearly defined and assigned information-security roles and responsibilities.* An effective cybersecurity program must be managed at the senior executive level and executed by qualified personnel.
5) *Strong access control procedures.* This helps guarantee that users are who they *say* they are. It also ensures that they have access to the data they seek. These access privileges should be reviewed at least every three months and disabled or deleted in accordance with a clear policy.
6) *Cloud-stored data-security reviews and independent assessments.* Because cloud computing raises unusual security concerns, employers must be able to evaluate how a third-party cloud service provider operates. Protections should include certain minimum provisions, such as multi-factor authentication and encryption procedures.
7) *Cybersecurity awareness training for all personnel.* Because employees can be the weakest link in cybersecurity, frequent training on identify theft and current trends in security breaches is essential.
8) *Secure System Development Life Cycle Program.* Such programs ensure that regular vulnerability assessments and code review are integrated into any system development. Best practices include requiring validation if a distribution is requested following changes to an individual's personal information, or if a request is made to distribute an individual's entire account balance.
9) *Business Resiliency Program.* Providers need to quickly adapt to disruptions while keeping assets and data safe. Core components of an effective program include a business continuity plan (for business functions), a disaster recovery plan (for IT infrastructure), and an incident response plan (for responding to and recovering from security incidents).
10) *Encryption of sensitive data stored and in transit.* This includes encryption keys, message authentication, and hashing (which can be used, for example, to avoid storing plaintext passwords in a database).
11) *Strong technical controls.* Best security practices include robust (and current) antivirus software, intrusion detection, firewalls, and routine data backup.

12) *Responsiveness to cybersecurity incidents or breaches.* Prompt action should be taken to protect the plan, including notifying appropriate agencies and individuals (e.g., law enforcement, insurer, participants), investigating the issue, and fixing the problem.

Online Security Tips

The final installment of EBSA's three-part release gives practical pointers that retirement account owners can use to reduce cybersecurity risk. Some tips are fairly self-evident reminders about creating and protecting passwords, avoiding free Wi-Fi networks, and recognizing phishing attacks. Some other tips may not be so obvious—and they bear mentioning here.

- Register, set up, and routinely monitor online accounts for retirement plans. Failing to register for an online account may enable cybercriminals to assume an account owner's online identify. Account owners that regularly check their accounts can help detect and respond to fraudulent activity.
- Use multi-factor authentication. This requires a second credential (like texting or emailing a code) to verify the account owner's identity before an inquiry or transaction is allowed.
- Keep personal contact information current. Account owners should ensure that their contact data includes multiple ways to reach them (by phone, text, or email). This will enable more effective communication if there is a suspected security breach.
- Close unused accounts. Even dormant accounts can contain personal information. If an account isn't needed, close it. Why give fraudsters the opportunity to steal data?

Next Steps

The previously mentioned GAO report also recommended that the DOL formally state whether cybersecurity is a fiduciary responsibility under ERISA. The DOL declined. It stated that fiduciaries must already "take appropriate precautions to mitigate risks of malfeasance to their plans, whether cyber or otherwise." Instead, the DOL identified minimum expectations for reducing cybersecurity risks, which should be undertaken by all private-sector employer-sponsored defined contribution plans.

This best-practice guidance (and other tips) does not specifically apply to other types of plans. Nevertheless, prudent employers, financial organizations, and service providers should certainly consider this guidance when determining their approach to cybersecurity for other plans, such as IRAs and healthcare plans. Any time that an entity maintains access to personal information of clients, it must rigorously protect that data. Adhering to EBSA's cybersecurity best practices is a good place to start.

Ascensus will continue to monitor future guidance on this subject and on other retirement and healthcare plan topics. Visit FuturePlan.com for future updates.