MAYNARD
COOPER GALE

Cybersecurity for
Retirement Plans and Their Participants

The release of what the Department of Labor has described as "compliance assistance materials" follows a recommendation by the Government Accountability Office (GAO) to provide guidance on minimum expectations for mitigating cybersecurity risks in ERISA-governed defined contribution plans. As data breaches continue to proliferate across the universe of electronic information systems, 401(k) and other individual account balance plans are tempting targets. Increased attention on cybersecurity will benefit fiduciaries and plan service providers, but the ultimate winners are participants and their beneficiaries.

The Employee Benefits Security Administration (EBSA) published the compliance tips in three documents entitled *Cybersecurity Program Best Practices* (aimed at recordkeepers and other service providers with electronic data and access), *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* (aimed at plan sponsors and other plan fiduciaries), and *Online Security Tips* (aimed at participants). The three documents complement each other, and effectively memorialize the minimum standards service providers are now expected to maintain in their cybersecurity programs. Perhaps the biggest win here is that the publications give plan sponsors and other fiduciaries a regulatory stick to demand change from service providers who are not adequately mitigating cybersecurity risks.

Cybersecurity Program Best Practices

The Cybersecurity Program Best Practices publication provides a substantive, practical reference tool for use by recordkeepers and other service providers in developing an effective cybersecurity program. While directed at service providers, *Cybersecurity Program Best Practices* has the dual effect of educating plan sponsors and other fiduciaries charged with hiring and monitoring recordkeepers. The best practices listed in the document set minimum standards of care:

1. Establish a **formal, documented cybersecurity program**. Regardless of the size of the plan being serviced, a recordkeeper or other service provider needs a written program which is understandable, communicated to relevant users (internally at the service provider level and externally at the plan sponsor and participant levels, as needed), and periodically reviewed and approved by senior leadership. The resulting policies and procedures should be comprehensive and address at a minimum items 2 through 12 listed below.
2. **Conduct prudent annual risk assessments** to identify where and how plan assets and participant data are stored on the system, the risks presented by the assets, data, and system, and the protocols developed and implemented to mitigate the risks.

3. **Engage an independent auditor to assess the provider's security controls**; maintain **written audit reports** and **document actions taken to correct problems identified in the audit**.
4. **Define and assign security roles and responsibilities to senior information security personnel.**
5. **Establish and maintain effective access controls** for authorized users with strong passwords, two-factor authentication, fraud detection procedures, and routine review of access privileges.
6. **Require a risk assessment for third-party cloud computing providers.**
7. **Conduct periodic (at least annually) cybersecurity training** focused on current trends and known weaknesses, including the risk of identity theft to obtain fraudulent distributions.
8. **Maintain a secure system development life cycle program (SDLC).** The service provider should test the system for external penetration attempts, conduct vulnerability scans, and test new or updated in-house or external modifications for weaknesses.
9. Develop and maintain a **written business continuity plan, disaster recovery plan and incidence response plan.**
10. Utilize **data encryption** while data is resting or transmitted when prudence dictates.
11. Use **up-to-date technical controls** in the system's hardware, software and firmware components, including such things as firewalls, antivirus software, and data back-up.
12. Take **appropriate action in response to cybersecurity breaches or incidents**, including notice to law enforcement, insurers, systems vendors, and affected participants. An incident should prompt an investigation and corrective action to prevent recurrence.

Tips for Hiring a Service Provider with Strong Cybersecurity Practices

The *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* publication reflects ERISA's general "prudence" standard in selecting service providers. At a minimum, a plan sponsor (or other fiduciary tasked with selecting or monitoring a service provider) should investigate the provider's cybersecurity policies and practices, its liability insurance coverage for data breaches, its track record in the industry, and how the provider has handled data breaches and incidents in the past. A prudent selection process also includes contract review; in particular, the provider should be contractually obligated to comply with recognized cybersecurity and information security standards. This publication provides leverage to plan sponsors tasked with persuading service providers to include contract terms enhancing cybersecurity protection for the plan and its participants, such as requiring a third party audit of the service provider's risk management (*e.g.*, a SOC 2 report), clear standards for use and disclosure of confidential information, prompt notice of cybersecurity breaches, compliance with record retention laws, and professional liability and E&O insurance protection against cybersecurity losses. Employers should also consider how providers evaluate their own security measures. Plan sponsors and other fiduciaries should use the twelve best practices listed above in evaluating a service provider's cybersecurity program.

Online Security Tips

The third publication, *Online Security Tips*, aims to educate plan participants and beneficiaries on common cybersecurity threats to reduce their risk of fraud and loss when accessing and managing their accounts. Plan sponsors may want to consider incorporating these tips into their own workforce or participant training. These best practices include:

- using two-factor authentication and unique and strong passwords;
- routinely monitoring electronic accounts and removing unused ones;
- installing antivirus software to protect against malware and other viruses; and

- avoiding free Wi-Fi networks (coffee shops, hotels, etc.) to check accounts.

The material also includes tips on phishing attacks and identity theft schemes, and provides helpful contact information to report cybersecurity incidents to the FBI and Homeland Security.

No matter your organization's role in the retirement industry, addressing cybersecurity risk is vital to mitigating the legal, regulatory, operational, reputational, and financial fallout that can accompany a security incident. The best practices promoted by the Department of Labor are ubiquitous across industries and mirror those adopted in guidance by other regulators (e.g., the Federal Trade Commission). Maynard Cooper has benchmarked hundreds of companies against these and other similar standards and requirements, and we would be happy to speak with you about how to effectively implement this guidance to become more cyber-resilient.

If you have questions or would like additional information about anything discussed in this Client Update, please contact a member of Maynard Cooper & Gale's Employee Benefits & Executive Compensation practice group.

This Client Alert is for informational purposes only and should not be construed as legal advice.
The information in this Client Alert is not intended to create and does not create an attorney-client relationship.