FIRST WATCH TECHNOLOGIES

Ullico INSURANCE | INVESTMENTS

3 KEY TAKEAWAYS

DOL CYBERSECURITY GUIDANCE FOR ERISA RETIREMENT PLANS

Retirement plan fiduciaries should review the guidance and consider using it to assess their own cybersecurity programs as well as evaluate the programs of their service providers. The guidance may also help plan fiduciaries with preparation to defend themselves against possible future claims brought under ERISA or data breach laws in the event of a service provider data breach. The following helps to summarize this recent guidance.

1 HIRING SERVICE PROVIDERS

The first part of the DOL guidance is directed to plan sponsors and plan fiduciaries and addresses how to evaluate a service provider's cybersecurity practices as part of their fiduciary duty.

- The guidance recommends that plan fiduciaries conduct due diligence by carefully reviewing and comparing the service provider's information security standards and practices
- Plan fiduciaries should consider how a service provider evaluates its cybersecurity practices, including whether it uses a third-party auditor to review its security practices on an annual basis. It also recommends plan fiduciaries evaluate a service provider's cybersecurity track record, including information about past security breaches, and inquire about the service provider's cybersecurity insurance.
- DOL advises that a plan fiduciary include various cybersecurity-related contract provisions in its agreements with service providers

2 CYBERSECURITY BEST PRACTICES

The second part of the DOL guidance provides cybersecurity best practices directed to record keepers and other service providers responsible for managing cybersecurity risks and to plan fiduciaries deciding which service providers to hire. Under the guidance, service providers should have a well-documented cybersecurity program that protects IT infrastructure, information systems, and data from both internal and external threats.

- The program should address cybersecurity processes that identify risks; protect systems and data; detect, respond to, and recover from cybersecurity incidents; and disclose incidents where required.
- Service providers' cybersecurity programs should be subject to review by a third party auditor and to annual risk assessments.
- For a cybersecurity program to be effective, it must be managed by senior leadership, such as a chief information security officer (CISO).
- DOL recommends that any data stored in a cloud-based service or managed by a third-party service provider be subject to security reviews and independent security assessments.
- The guidance also shares other recommendations ranging from cyber security awareness training for participants to encryption of sensitive data.

3 ONLINE SECURITY TIPS

The final part of the guidance offers plan participants and beneficiaries some basic tips to reduce the risk of fraud and loss:

- Register, set up, and routinely monitor your online accounts
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Use antivirus software and keep apps and software current
- Know how to report identity theft and cybersecurity incidents

IN CONCLUSION

Retirement plans maintain significant amounts of detailed personal and financial data. The companies and people who sponsor, service, and benefit from these plans can be considered prime targets for cyber attackers. Recent DOL guidance aims to encourage retirement plan fiduciaries to ensure their service providers, participants, and beneficiaries have the cybersecurity resources and tools in place to protect data and avoid potentially costly and damaging data breach incidents.