September 9, 2024

Services

Employee Benefits and Executive Compensation

Fiduciary Duties and Governance

Qualified Retirement Plans

Taft-Hartley Plans

Health and Welfare Plans

Government Plans

Higher Education

Employee Stock Ownership Programs (ESOPs)

Executive Compensation and Nonqualified Plans

ERISA Fiduciary and Benefits Litigation

College Savings and ABLE Plans

Mandatory Paid and Unpaid Leave

Audits and Investigations

U.S. Department of Labor Updates Cybersecurity Guidance for ALL Employee Benefit Plans

On September 6, 2024, the U.S. Department of Labor ("DOL") issued new guidance to help plan sponsors and fiduciaries safeguard plan-related data. The new guidance also clarifies that the DOL's cybersecurity guidance applies to ***all*** employee benefit plans, not just retirement plans.

Background

As discussed in our prior Client Alert, in 2021 the DOL issued a Compliance Assistance Release to provide cybersecurity best practices for plan sponsors, fiduciaries, recordkeepers and plan participants. Since then, health and welfare plan service providers have told DOL investigators that the 2021 guidance only applies to retirement plans. To address that issue, the DOL issued a new Compliance Assistance Release to clarify that its cybersecurity guidance applies to ***all*** employee benefit plans subject to ERISA, including health and welfare and pension plans.

Cybersecurity Guidance

The Compliance Assistance Release focuses on three areas: tips for hiring service providers, cybersecurity program best practices, and online security tips for plan participants. While our prior Client Alert provides additional details, key tips include the following.

Best practices for hiring service providers include:

- Asking about the service provider's information security standards.
- Asking how a service provider validates its practices.
- Evaluating the service provider's track record in the industry.
- Asking whether the service provider has experienced past security breaches.
- Confirming the service provider has insurance policies that would cover losses caused by cybersecurity and identity theft breaches.

Cybersecurity program best practices include:

- Having a formal, well-documented cybersecurity program.
- Conducting prudent annual risk assessments.
- Having a reliable annual third-party audit of security controls.
- Clearly defining and assigning information security roles and responsibilities.
- Having strong access control procedures.
- Ensuring 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.
- Conducting periodic cybersecurity awareness training.
- Implementing and managing a secure system development life cycle (SDLC) program.
- Having an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
- Encrypting sensitive data, stored and in transit.
- Implementing strong technical controls in accordance with best security practices.
- Appropriately responding to any past cybersecurity incidents.

Next Steps

The DOL's new Compliance Assistance Release suggests that the DOL will increase its focus on data privacy/security issues when conducting audits or investigations on ***all*** employee benefit plans. We have already seen this activity with retirement plans, and we expect to see much more activity with respect to health and welfare plans. To help address cybersecurity issues, plan sponsors and fiduciaries should:

- Require ***all*** service providers to provide details on their information security practices and independent audits confirming compliance.
- Require service providers to agree to data privacy/security requirements in their service agreements, including provisions relating to breach notifications and mitigation.
- Ensure service provider contracts include insurance and indemnification obligations relating to data privacy and security breaches and incidents.
- Periodically review service providers' compliance with their agreements and document that process.
- Prepare, document, implement, and periodically review and update cybersecurity policies, procedures, and programs for ***all*** employee benefit plans.
- Provide periodic training to all employees on privacy and security best practices.

If you have questions about the cybersecurity guidance or the compliance obligations created by the guidance, please contact a member of Kutak Rock's Employee Benefits and Executive Compensation practice group.

Contacts

John E. Schembari
Omaha
402.231.8886
john.schembari@kutakrock.com

Michelle M. Ueding
Omaha
402.661.8613
michelle.ueding@kutakrock.com

William C. McCartney
Omaha
949.852.5052
william.mccartney@kutakrock.com

P. Brian Bartels
Omaha
402.231.8897
brian.bartels@kutakrock.com

Ruth S. Marcott
Minneapolis
612.334.5044
ruth.marcott@kutakrock.com

Sevawn Foster Holt
Little Rock
501.975.3120
sevawn.holt@kutakrock.com

John J. Westerhaus
Omaha
402.231.8830
john.westerhaus@kutakrock.com

Robert J. Hannah
Omaha
402.661.8667
robert.hannah@kutakrock.com

Marcus P. Zelzer
Minneapolis
612.334.5037
marcus.zelzer@kutakrock.com

Emma L. Franklin
Omaha
402.231.8842
emma.franklin@kutakrock.com

Aaron D. Schuster
Kansas City
816.960.0090
aaron.schuster@kutakrock.com

Jacob S. Gray
Minneapolis
612.334.5053
jacob.gray@kutakrock.com

Jason Kotlyarov
Kansas City
816.502.4622
jason.kotlyarov@kutakrock.com