King & Spalding
Client Alert

JUNE 21, 2021

For more information, contact:

Jake Downing
+1 312 764 6935

Jeanie Cogill
+1 212 556 2161

Sumon Dantiki
+1 202 626 5591

Alexis Rosett
+1 212 790 5301

King & Spalding

Chicago
110 N Wacker Drive
Suite 3800
Chicago, IL 60606
Tel: +1 312 995 6333

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

The Department of Labor Issues its First Cybersecurity Guidance for Plan Sponsors, Fiduciaries and Service Providers

Issue 10: 10 in 10

It's been, as the song goes, a long, long time coming. In April, the Department of Labor issued its first ever formal cybersecurity guidance for retirement plan sponsors and retirement plan fiduciaries, and for the service providers they hire to assist them. The three-part guidance follows some serious prompting over the last decade from the ERISA Advisory Council and from the GAO, who warned of the cybersecurity risks to employee benefit plan administration and urged the Department of Labor to establish minimum expectations for managing and mitigating these risks. And with good reason – ERISA-covered retirement plans hold some $9.3 trillion in assets, so the potential value of personally identifiable information or "PII" housed in the servers of employers, recordkeepers, trustees and others is immense. And frequently multiple unrelated entities, not to mention the employees and beneficiaries themselves, have access to sensitive employee data and asset information as an ordinary part of the benefit plan administration process.

Employers with operations outside the United States are already subject to more stringent regulatory data privacy and security requirements (e.g., the European Union's General Data Protection Regulation) and these more stringent data privacy and security requirements often already impact U.S. retirement plans with participants residing outside the United States.

Further, many companies have already established data privacy and security protocols that go beyond what was technically required under current Department of Labor guidance and have applied these protocols to their retirement plan programs.

As a result, the new guidance more closely aligns the data privacy and security requirements of United States retirement plans with the requirements outside the United States and with general corporate standards.

The guidance is based on the central premise that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks."

Tips for Hiring a Service Provider with Strong Cybersecurity Practices. This guidance identifies six cybersecurity considerations – designated as "tips" - to help plan sponsors and fiduciaries prudently select and monitor recordkeepers and other service providers. The first five outline the employer's fiduciary diligence process, and reflect ERISA's familiar "process driven" approach (e.g., employers should ask about the service provider's information security standards and audit results and compare them to the industry standards adopted by other financial institutions. The sixth "tip" encourages plan fiduciaries to include certain covenants in the contract with a service provider, including ongoing compliance with cybersecurity and information security standards, timely notification of and attention to cybersecurity breaches, and maintenance of adequate cyber liability and data privacy breach insurance. The tips also caution against contract provisions that limit the service provider's responsibility for IT security breaches.

Cybersecurity Program Best Practices. This document identifies twelve "best practices" for plan service providers. Again, some recommendations outline a "prudent process," such as having periodic workforce cybersecurity training, but others are more prescriptive. For example, one "best practice" calls for encryption of sensitive data "stored and in transit," another for an annual independent third-party audit of the service provider's security controls, another for annual cybersecurity awareness training for the workforce. And plan sponsors should note that, although this portion of the guidance addresses best practices for "recordkeepers and other service providers responsible for plan-related IT systems and data," the guidance is also squarely aimed at plan fiduciaries responsible for "making prudent decisions on the service providers they should hire."

Takeaways for Employers, Fiduciaries and Service Providers. The guidance has been issued just at the start of a trend in litigation against retirement plan sponsors and fiduciaries and service providers for participant losses from cybersecurity lapses. As a result, concerns have been raised that the guidance could create a blueprint for plaintiffs' lawyers, who may assert that the guidance, although presented as "tips" and "best practices," sets out not recommended approaches but minimum standards that plan fiduciaries must meet in order to ensure the security of participant data. If so, a fiduciary's failure to meet one of the recommended steps - for example, failing to include a particular contract term in a recordkeeping agreement – could be framed as a breach of fiduciary duty. But employers and service providers may likewise limit their exposure by hewing closely to the steps recommended in the guidance. Employers and administrators should therefore review their current cybersecurity practices and service provider contracts and evaluate whether they meet the suggested standards. Recordkeepers, directed trustees and others whose systems hold, modify and transmit retirement plan participant data should similarly compare their current cybersecurity policies and procedures against the best practices outlined by the new guidance. As noted at the outset, many employers and services providers were well ahead of the Department of Labor on implementing cybersecurity procedures and the guidance may just provide an opportunity for a quick check-up on already robust procedures.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MOSCOW	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	