CAPTRUST

An Early 2021 Surpriseâ€”Cybersecurity Guidance from the Department of Labor

A glaring regulatory hole in recent years has been the lack of guidance from the Department of Labor (DOL) on the emerging issue of cybersecurity, despite some high-profile cases of theft from participant retirement plan accounts. However, that changed on April 14, when the DOL issued guidance on best practices for maintaining cybersecurity, including tips on how to protect participants' retirement benefits.

The guidance comes as somewhat of a surprise, as it was not expected until later in the year and the new DOL secretary was only recently confirmed. However, it follows a March 15 report from the Government Accountability Office (GAO) that urged the DOL to expedite its timeline.

Following are some highlights from the DOL guidance:

- The DOL's service provider review suggestions range from the obvious—such as confirming that the provider is properly insured against participant account theft and asking about the provider's information security standards—to the more comprehensive—such as inquiring about past security breaches and the provider's response to them, along with seeking contractual confirmation of the plan sponsor's notification timeframe in the event of a breach. Though the DOL has communicated these as Tips for Hiring a Service Provider, plan sponsors should review the provisions with existing service providers that maintain plan records and participant data to confirm safeguards are in place.
- The DOL provides a 12-part menu of cybersecurity best practices for plan service providers, which includes implementing a formal and documented cybersecurity program, ensuring that assets or data stored in a cloud or managed by a third party are subject to independent security reviews and assessments, and encrypting sensitive data.

- The DOL provides tips for participants to help protect their own data and dollars, such as registering online accounts, regularly checking account status, using strong and unique passwords, avoiding free Wi-Fi, and reviewing information on identifying and avoiding phishing attacks. Plan sponsors should consider communicating these tips to their participants on a regular basis.

The guidance is concise and practical, offering a variety of best practices. Plan fiduciaries should pay special attention to this guidance and act accordingly to prevent cybersecurity breaches and theft from their retirement plans.