KILPATRICK TOWNSEND

April 19, 2021

DOL Releases Cybersecurity Guidance

by R. Sterling Perkinson , Peter Daines

On April 14, 2021, the Department of Labor ("DOL") issued several pieces of guidance on cyber security best practices, including: (1) a press release, (2) Online Security Tips for retirement plan participants, (3) a Tips for Hiring a Service Provider with Strong Cybersecurity Practices, and (4) Cybersecurity Program Best Practices. This set of cybersecurity guidance emphasizes how critical it is for fiduciaries to focus on cybersecurity issues in selecting, contracting with and monitoring the performance of recordkeepers and other plan service providers to protect plan participants. Fiduciaries should focus on cybersecurity in performing service provider due diligence, in negotiating service provider contracts, and in ongoing monitoring of a service provider's compliance with policies and procedures and to ensure that any breaches are promptly reported, investigated and addressed.

Cybersecurity and Fiduciary Duties

The ERISA fiduciary standards require that a plan be administered in accordance with a standard of care for a prudent person who is familiar with such matters. Accordingly, ERISA fiduciaries must ensure that a plan's administration is in accordance with industry standards for cybersecurity in the financial services industry. Fiduciaries have a responsibility to safeguard plan assets, and so they must ensure that controls are in place to avoid financial losses to plans that may result from a cybersecurity breach.

Breaches of participant data due to cybersecurity incidents could also implicate fiduciary duties to the extent that participant data are considered "plan assets," as has been challenged in some recent litigation. These cases involve claims that participant data has been improperly used for purposes other than plan administration, such as for marketing of other services. The limited number of courts that have ruled on the issue applied ordinary principles of property law to conclude that participant data is not a plan asset. Divane v. Northwestern University, 2018 WL 2388118 (N.D. Ill. 2018), aff'd, 953 F.3d 980 (7th Cir. 2020); Harmon v. Shell Oil Co., 2021 WL 1232694 (S.D. Tex. March 30, 2021). However, the issue remains an open question in most jurisdictions.

Cybersecurity Considerations for Fiduciaries

The DOL's cybersecurity guidance affirms the importance of taking cybersecurity into consideration when fiduciaries are selecting, contracting with and monitoring recordkeepers or other plan service providers. In particular, the "Tips for Hiring a Service Provider with Strong Cybersecurity Practices" encourages fiduciaries to

address cybersecurity as follows:

- Due Diligence. In selecting a service provider, fiduciaries should review the service provider's cybersecurity policies and procedures to assess how they compare to industry standards. This includes:
    - o Confirming whether third party audits are performed and reviewing any audit reports;
    - o Inquiring about any security incidents and what steps have been taken in response to them;
    - o Reviewing public information, including litigation records, regarding any cybersecurity incidents involving a service provider; and
    - o Assessing levels of cybersecurity or identity theft insurance policies and levels of coverage.

- Contract Provisions. Contracts with service providers should:
    - o Require the service provider to obtain a third party audit to assess compliance with policies and procedures;
    - o Prohibit the use or sharing of participant information without consent and generally meet a strong standard of care for protecting the information;
    - o Require prompt notification in the event of any cyber incident or data breach and cooperation to investigate and address the cause of the breach;
    - o Require compliance with privacy laws and regulations regarding the privacy and security of participant information; and
    - o Require appropriate levels of professional liability and errors and omissions insurance, cyber liability and privacy breach insurance and other fiduciary bond or blanket crime insurance.

The DOL's "Cybersecurity Best Program Practices" describe what the DOL believes to be best practices and procedures for service providers. Plan fiduciaries can use this as a reference in evaluating the cybersecurity practices and procedures of potential service providers.

Fiduciaries may also want to ensure that the "Online Security Tips" are shared with individual participants or similar information is provided by the plan's recordkeeper or other service provider.