SCHNEIDER DOWNS
Wealth Management

Department of Labor Guidance for Cybersecurity

Department of Labor has issued guidance in the form of "Tips" and "Best Practices" for cybersecurity. Plan Sponsors should be prepared to establish on audit that they have done their due diligence regarding cybersecurity.

- In April, the Department of Labor issued its first guidance on cybersecurity for plan sponsors, service providers and participants. It did so at the behest of the Government Office of Accountability (the "GAO"). That agency has been pushing the Department to identify minimum standards for mitigating cyber security risks in benefit plans.
- Although cyber threats are a relatively new phenomenon, these threats simply throw a new wrinkle into the longstanding obligation of plan fiduciaries and service providers to safe keep plan assets. Cybersecurity has been a priority in the financial service industry for some time and measures to prevent cyber breaches come on top of many longstanding security protocols in place to protect customer accounts.
- The recommended steps in this guidance are obvious and are things the industry, by and large, is already doing. However, this guidance is worthwhile as it clarifies what the Department of Labor expects from fiduciaries with regard to cybersecurity.
- While this guidance is framed as "tips" and "best practices," it should view as setting minimum standards for plan fiduciaries and service providers in mitigating cyber threats. In future litigation concerning cyber breaches, there is no doubt the courts will look to this guidance in deciding if plan fiduciaries acted prudently and to determine the responsibilities of the respective parties. The practical consequence of this guidance is it makes clear (if there was ever a question about this) that plan fiduciaries must do due diligence around and be informed about the measures service providers are taking to prevent cyber breaches of their systems. While many sponsors have done some due diligence around the cybersecurity, the majority will now need to do a deeper dive to ensure they are complying with this guidance.

The guidance consists of three sperate documents

Tips for Hiring a Service Provider with Strong Cybersecurity Practices. Most of these tips are rather obvious and include understanding and knowing:

- The service provider's security measures and knowing these are consistent with industry standards;
- The service provider's track record for breaches;
- There is an independent audit establishing that effective security measures are in place and are being followed; and
- Reviewing the service contract to ensure that it explicitly states that the service provider is fully responsible for cyber breaches.

Cybersecurity Program Best Practices. These are 12 points that recordkeepers and other service providers should follow which again are obvious and are all steps that established companies in financial services industry are most likely already taking. These include:

- The cybersecurity program is well documented;
- An annual audit by an independent third party that establishes effective security measures are in place and are being followed; and
- Employee training on security measures.

Continued on back

Online Security Tips. These tips are directed at participants and again are obvious such as the importance of strong passwords, monitoring accounts regularly and not falling for phishing attacks. The significance is these tips acknowledge that participants, often their own worst enemy when it comes to security, have some responsibility in keeping their account secure and have an obligation to follow security protocols.

- Plan sponsors must now be prepared in a Department of Labor audit to establish that they have done the necessary due diligence around cybersecurity and record keepers must now be prepared to show there are effective programs in place to prevent cyber breaches. Investigations are already underway where the Department has requested significant documentation regarding cyber security including items such as written policy and procedures, risk assessments and cyber security awareness training.