Retirement Plan Cybersecurity: Truth, Justice, and the DOL Way

August 2, 2021

At a time when digital security and cyberattacks are key concerns for individuals and businesses alike, plan sponsors and other plan fiduciaries have a key role to play in protecting retirement plan assets and data. Otherwise known as "responsible plan fiduciaries," these individuals and certain plan service providers have a fiduciary duty to ensure there is a robust cybersecurity program in place to keep plan assets and data secure.

As we previously reported on our blog here, the DOL recently issued guidance in this arena to keep employers and plan fiduciaries compliant. The DOL is now specifically targeting employers and plan fiduciaries who fail to adequately protect employee retirement plan assets from hackers and cyberthieves, so the time to act is before the DOL issues a plan audit and before participants are victimized by cybercriminals or hackers.

The DOL requires that plan fiduciaries responsible for prudently selecting and monitoring service providers ensure these allies maintain strong cybersecurity practices. To assist in this process, the DOL has published a checklist of twelve cybersecurity program best practices for ERISA plan service providers to follow. Not only should responsible plan fiduciaries be familiar with these cybersecurity best practices, they should also ensure their plan service providers adhere to these best practices as well. To do this, responsible plan fiduciaries should implement ***and document*** a prudent process to ensure that existing service providers are protecting plan data and assets from cybercriminals. As part of this process, responsible plan fiduciaries should:

- Ask about the service provider's information security standards, practices and policies, and audit results, and then compare them to industry standards.
- Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented.
- Evaluate the service provider's track record, including public information regarding information security incidents and litigation.
- Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
- Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity or identity theft breaches.
- Review the contract with the service provider to ensure it requires ongoing compliance with cybersecurity and information security standards.
    - The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.
    - The contract should meet a strong standard of care to protect confidential information and clearly describe the service provider's obligations to prevent the unauthorized use or disclosure of confidential information.
    - The contract should identify how quickly the plan fiduciary will be notified of any cyber incident or data breach.
    - The contract should ensure the service provider's cooperation to investigate and reasonably address the cause of the breach.

- The contract should expressly state the service provider's obligations to comply with all applicable federal, state, and local laws, rules, regulations, directives, and other governmental requirements pertaining to the privacy, confidentiality, or security of participants' personal information.
- The DOL also recommends that plan fiduciaries be wary of contract provisions that limit the service provider's responsibility for cybersecurity breaches.

By implementing a prudent process to ascertain service provider compliance with cybersecurity best practices, not only will responsible plan fiduciaries be better prepared to save participants from the dastardly schemes of cybercriminals, but also to ward off potential fiduciary breach claims from the DOL and victimized participants; a truly heroic outcome for participants and employers alike.

A list of the twelve "Cybersecurity Program Best Practices" identified by the DOL is available here.