Retirement plan sponsors and fiduciaries now have one more responsibility – *cybersecurity*

4.20.2021

For many years, group health plans have been subject to strict privacy and security requirements, but up to now, privacy and security for retirement plans has been left to the vagaries of the plan service providers and their auditing systems. The U.S. Department of Labor ("DOL") has now issued informal "tips" and "best practices" for maintaining cybersecurity for retirement plans. Not surprisingly, under this guidance, the burden falls on plan sponsors and plan fiduciaries to select retirement plan service providers with strong cybersecurity practices, and to monitor the cybersecurity practices of existing plan service providers. Plan fiduciaries should assess the strength of the cybersecurity practices of each plan service provider with access to plan data and amend their service agreements as necessary. The adequacy of any insurance coverage for liability resulting from fiduciaries' new cybersecurity monitoring responsibilities should be evaluated, along with plan fidelity bond coverage.

Background

Hackers have penetrated the electronic security systems of many major ***federal governmental agencies*** (e.g., U.S. Office of Personnel Management: 21.5 million affected; U.S. Voter Database: 191 million affected; U.S. Department of Veteran Affairs: 26.5 million affected), ***of state agencies*** (e.g., Georgia Secretary of State Office: 6.2 million affected; Office of the Texas Attorney General: 6.5 million affected; Virginia Department of Health Professions: 8.3 million affected), ***and of major companies*** (e.g., Yahoo: 3 billion compromised accounts; First American Financial Corp.: 885 million records; Facebook: 540 million user records; Marriott International: 500 million guests).

According to one source, an average of 4,800 websites a month are compromised with code that steals the data entered into their forms, and the average time to identify a breach in 2020

Related People

Robert B. Stevenson
Of Counsel

Related Services

Cybersecurity and Privacy Specialty Team

Employee Benefits

was 228 days, while the average time to contain a breach was 80 days.

Recognizing that retirement plans in the U.S. hold more than $9.3 trillion in assets - making them prime targets for cyber criminals – the DOL compiled a list of "tips" to help plan sponsors and fiduciaries *"prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires."* Additionally, the DOL prepared a list of "best-practices" for use *"by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire."*

Implicit in these tips and best practices is the DOL's opinion that plan fiduciaries are responsible for taking prudent steps to ensure that their plan service providers – including *current* plan service providers holding or accessing sensitive data – take appropriate measures to protect plan data from cybertheft.

Ironically, recent court decisions have held that a retirement plan's data is not a "plan asset" under the Employee Retirement Income Security Act ("ERISA"), entirely ignoring the fact that the data is extremely valuable – the data contains the proverbial keys to the kingdom.

Tips for Hiring or Monitoring a Service Provider

There are a number of DOL-suggested "tips" for hiring a service provider with strong cybersecurity practices. Among those are:

- Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity.

This may be reflected in the service agreement as an obligation to maintain a global cybersecurity certification from an independent organization and an obligation to obtain a SOC 2 and SOC Cybersecurity audit each year, and to provide copies of each audit report implicating plan data.

- When you contract with a service provider, beware of contract provisions that limit the service provider's responsibility for IT security.

Since plan fiduciaries have no ability to directly protect the plan data in the service provider's possession, its reasonable that the service provider must be the party to assume liability for its failure to prudently protect that data. The service provider can obtain insurance to cover the risk that it will fail to meet its obligations.

- Try to include terms in the contract that would enhance cybersecurity protection for the Plan and its participants, such as prohibiting the use or disclosure of confidential information without written permission.

When a plan service provider is given a contractual right to use plan data for its own marketing purposes, or for purposes of marketing products from related companies, the dispersion of plan data across multiple entities increases the risk of a security breach.

There are several other "tips" in the DOL guidance. It is important to ask your ERISA attorney to review the terms of your existing service provider agreements to determine whether they can and should be amended in light of these new DOL "tips."

Best Practices

The new DOL "Cybersecurity Program Best Practices" state that "plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks." While the best practices are intended to be used by recordkeepers and other service providers responsible for plan-related IT systems and data, they are also intended to provide a litmus test that plan fiduciaries may use in order to prudently select and monitor the plan service providers.

The list of best practices is lengthy and should be reviewed carefully, but it includes things such as:

- A prudent annual risk assessment should be performed to identify, estimate, and prioritize information system risks.
- A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.
- The service provider should periodically assess its own third party service providers based on potential risks.
- Cybersecurity awareness training for all personnel should be conducted at least annually and should be updated to address risks identified by the most recent risk assessment.

A plan fiduciary will need to engage with their plan service provider to gather the information necessary to form a prudent opinion regarding whether the service provider complies with these best practices. As was the case with the DOL tips, it is important to ask your ERISA attorney to review the terms of your existing service provider agreements to determine whether they can and should be amended in light of these new DOL "best practices."

Conclusion

Plan fiduciaries should now contact their existing plan service providers that have access to sensitive plan data, to determine whether the service provider is in fact following the new DOL "best practices." By documenting the service provider's compliance with these best practices, plan fiduciaries can help avoid incurring personal liability for losses resulting from a data security breach. This documentation is also likely to be added to the list of documentation requested by the DOL in the event of an audit.

If the plan administrator has access to sensitive plan data and provides services in a fiduciary capacity, they should also follow these best practices to the extent applicable.

Additionally, each service agreement should contain requirements that the service provider will follow, at minimum, the "best practices" identified by the DOL. This means that whenever possible, existing contracts should be amended, and new contracts should be negotiated to address these cybersecurity concerns.

Moreover, companies should review the scope of their fiduciary liability coverage to determine whether it is adequate to protect the plan in the event of a cybersecurity breach. Fiduciary liability coverage that includes coverage for cybertheft should be in place, to protect the fiduciaries from personal liability resulting from an alleged failure to prudently select or monitor plan service providers that have access to sensitive plan data.

Contact the author or any Butzel Long employee benefit attorney for help in addressing your new cybersecurity responsibilities, including:

- Reviewing and revising existing service provider agreements;
- Reviewing fidelity bond coverage terms to assess coverage for cybertheft oversight duties;
- Reviewing fiduciary liability insurance coverage terms to assess coverage for cybersecurity oversight duties;
- Prepare cybersecurity policies and procedures; and
- Preparing notices to participants regarding cybersecurity measures they should be taking to protect their plan data and benefits.

Lynn McGuire
734.213.3261
mcguire@butzel.com

Thomas L. Shaevsky
248.258.7858
shaevskey@butzel.com

Andrew Stumpff
734.213.3608
stumpff@butzel.com

Mark Jane
734.213.3617
jane@butzel.com

CLIENT ALERTS

Robert B. Stevenson
734.213.3436
stevenson@butzel.com

Nancy Keppelman
734.213.3433
keppelman@butzel.com

Diane M. Soubly
734.213.3625
soubly@butzel.com

Alexander B. Bragdon
248.258.7856
bragdon@butzel.com