WINSTON & STRAWN LLP

BLOG

Best Practices in Providing Cybersecurity for 401(k) Accounts Continue to Advance

OCTOBER 12, 2018

Given the times, It is no longer atypical for clients to experience situations involving the theft of participants' retirement account balances as the result of a variety of criminal methods, including "phishing" emails, participants' carelessness in protecting their passwords, family theft, etc. And, while the employer's cyber-insurance coverage may cover litigation costs associated with the breach, such policies typically will *not* restore the participants' underlying accounts balances.

We have previously written on the steps that prudent plan fiduciaries should take to protect their retirement plans from the risk of a cyberattack. In two reports, one from 2011 and one from 2016, the Department of Labor's ERISA Advisory Council has provided a roadmap. Those reports make it clear that, while it is nearly impossible to eliminate all cybersecurity risks, prudent plan fiduciaries should actively seek to manage those risks.

Managing that cybersecurity risk requires establishing a process that includes implementing, monitoring, and testing access to and retention of data. That can involve actions such as: (1) having the employer's cybersecurity lawyers review the provisions in all contracts with third parties that involve access to plan participants' data; (2) having the company's internal or external auditors test the plan systems to identify potential weakness that could lead to a cyber-attack; and (3) regularly updating the plan's fiduciary committee about the plan administrator's cybersecurity efforts—both what has been done and what will be done next.

Thankfully, new tools may be available to help plan sponsors provide participants with additional protections against a cyberattack. Many large third-party recordkeepers have recently unveiled programs pursuant to which the vendor will restore the participants' accounts in the event of a cyber-attack. Given how rapidly these programs are evolving, all recordkeepers will be under significant competitive pressure to have some type of offering. As a result, it is likely that best practices for plan fiduciaries regarding cybersecurity will require the fiduciaries to ask questions along the following to their existing service providers and in requests for proposals:

1. Does our [or our potential] 401(k) plan recordkeeper offer a program to restore these accounts?
2. What are the limits of the coverage (either per participant, per attack, per plan)?
3. Are there any deductibles before the coverage kicks in?
4. What things are not covered? Specifically, can certain actions (or inaction) by the participant void the coverage?

5. What must the participant do to activate the coverage? Recordkeepers' policies require participants to do such things as: register the device they will use to access the website, check account statements regularly, sign up for electronic delivery of statements, allow for text messages, notify the recordkeeper of address or email changes, etc.
6. To the extent participant action is required, how to best communicate to participants. Timing can be a factor in notifying someone that a distribution request has been received with respect to their account balance. In addition, such communications will need to be thoughtfully drafted to carefully underscore the risk while announcing the protection offered by the new program and the necessary steps for the participants to access such coverage.

As the strategies of cybercriminals continue to evolve, plan fiduciaries must continually review and update their policies and protocols to ensure that they are prudently addressing this incredibly significant risk, including by exploring available cybersecurity guarantees from recordkeepers.

2 Min Read

Authors

Joseph S. Adams

Amy Gordon

Related Locations

Chicago

Related Topics

Cyber Security

401(k)

Related Capabilities

Employee Benefits & Executive Compensation

Related Regions

North America

Related Professionals

Joseph S. Adams

Amy Gordon

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.