JOURNAL of PENSION BENEFITS

Issues in Administration, Design, Funding, and Compliance
Volume 27 • Number 2 • Winter 2020

Your Plan Has Been Hacked, Now What?—Next Steps for Retirement Plan Sponsors Following a Cyberattack

By Ryan Gorman and Elizabeth "Bess" Hinson

Ryan Gorman is an associate in the Employee Benefits & Executive Compensation Practice Group at Morris, Manning & Martin in Atlanta, GA, where he regularly counsels employers regarding ERISA fiduciary matters and employee benefit plan administration issues. Mr. Gorman assists his clients with the design, implementation and compliance initiatives of qualified retirement plans, executive compensation arrangements, severance programs, and health and welfare arrangements. In addition, he represents clients in the employee benefits and executive compensation aspects of mergers, acquisitions, financings, and other types of transactions, including post-transaction benefits integration.

Elizabeth "Bess" Hinson is a partner-elect at Morris, Manning & Martin LLP in Atlanta, GA. As Chair of the Cybersecurity & Privacy Practice, Ms. Hinson makes planning for privacy and cybersecurity risks her top priority. Her primary areas of concentration include cyber and data risk management and governance, breach preparedness and response, crisis management, and global data privacy compliance.

Once a threat, or incident, or cyberattack has been identified, it is of the utmost importance for retirement

plan sponsors and fiduciaries to actively engage all stakeholders and legal counsel, and document the steps taken. The action to take in response to such a cyberattack depends on whether the incident occurred on a first-party system or a third-party system.

As of March 31, 2019, the value of private sector retirement plan assets in the United States exceeded $11.31 trillion, a figure that includes both private employer-sponsored defined contribution plans (*e.g.*, Internal Revenue Code Section 401(k) plans, 403(b) plans, and 457 plans) as well as private employer defined benefit plans. ["The US Retirement Market, First Quarter 2019," Investment Company Institute, Federal Reserve Board, and Department of Labor. *https://www.ici.org/info/ret_19_q1_data.xls* (retrieved August 2019)] This represents a $6 trillion increase in assets over the last 10 years.

As access to retirement plan accounts becomes more and more digitized, cyber criminals increasingly are targeting retirement funds and the underlying data associated with participant accounts. Many retirement plan sponsors and third-party vendors have taken actions to protect retirement plan accounts from these nefarious actors, as the accounts contain valuable data and personally identifiable information, including names, addresses, Social Security numbers, birthdates, and bank account information (relating to direct deposit/payroll feeds). Cyber criminals in this area are incredibly sophisticated, and known examples of cyberattacks include efforts to request fraudulent distributions or loans from plan accounts, redirecting direct deposits or mailing addresses for purposes of distributions from plans, and ransomware/phishing attacks that result in a breach of personal information. Clearly, the stakes have never been higher for employers with respect to securing retirement plan assets and data.

Employers are becoming well-versed in best practices in cybersecurity, but even the most prepared employers and third-party vendors can be subject to cyberattacks on retirement plans. The reality is that these attacks can and will occur—but once an attack has occurred, what should plan sponsors keep in mind and do next?

Promptly Engage Outside Legal Counsel and Follow Your Script

Upon discovery of a breach or theft, the plan sponsor should promptly engage outside legal counsel in order to protect any information related to the incident or the investigation of the incident under the attorney-client privilege.

To the extent that the plan sponsor or legal counsel has a documented process for what to do in the event of a breach, it should be followed and the response should be documented. Time and legal were likely involved in developing that process, so it should be followed. In addition, some state breach notification laws require employers to retain a written determination of a data breach and supporting documentation after the breach has been detected, and state attorneys general may have a statutory right to request that the employer produce the documentation. For example, Arkansas recently adopted a data breach notification law, and Florida has existing strict regulations of breach notification. [*See* Arkansas Personal Information Protection Act HB 1943, Arkansas Code §4-110-103(7); Florida Information Protection Act of 2014, Fla. Stat. §501.171]

Remember the Responsibilities Unique to Retirement Plans

Despite growing concern from activist groups and increasing attention from Congress about retirement plan cyber threats [February 12, 2019, Letter to U.S. Government Accountability Office from Chairman of House Committee on Education & Labor and Senate Committee on Health, Education, Labor & Pensions, *https://www.help.senate.gov/imo/media/doc/190212%20GA0%20Retirement%20Cybersecurity%20Request.pdf* (retrieved August 2019)], current federal laws governing retirement plans do not directly address cybersecurity. Indeed, there is no equivalent to the privacy and security regulations applicable to employer-sponsored group health plans under the Health Insurance Portability and Accountability Act (HIPAA). Instead, retirement plan sponsors and other individuals with control over management of plan assets must adhere to the general fiduciary standards of the Employee Retirement Income Security Act of 1974, as amended (ERISA).

Because these standards were introduced before the threat of cyberattacks on retirement plans, the application of ERISA is somewhat open to interpretation. When considering the differences between a cyberattack on retirement plans versus a cyberattack

on employers generally, however, it is clear that plan sponsors are bound by a higher standard to address the cyberattack in a diligent manner. This is because ERISA generally requires retirement plan fiduciaries to act prudently and in the best interest of plan participants and beneficiaries. As it relates to a breach of retirement plan accounts and/or data, this means that plan fiduciaries are required to actively engage in a response to a potential cyber theft or breach with a heightened level of expertise. Learning "on the fly" or pleading inexperience will not suffice, and plan fiduciaries must take actions to investigate, notify participants, correct breaches, and ensure breaches of a similar nature do not occur again in the same manner in which a prudent person with knowledge of the subject would under like circumstances. Fiduciaries also are responsible for monitoring the actions of service providers, so active engagement with third parties handling plan assets and data, as well as vendors brought in to remedy the breach or attack, is of vital importance as well. Lastly, documentation of the plan sponsor's response to a breach is pivotal for establishing and demonstrating the prudent actions taken should there be a subsequent challenge, audit, or complaint against the plan's stakeholders and fiduciaries.

Course of Corrective Action Depends on Details of Breach

There is a variety of stakeholders involved in the maintenance of a retirement plan and, as a result, various parties can have custody of retirement plan assets or maintain sensitive personally identifiable information. As a result, the proper course of response to a cyberattack relating to a retirement plan depends on whether the incident occurred on a first-party (*i.e.*, employer/plan sponsor) system or a third-party (*i.e.*, recordkeeper, custodian, or third-party administrator) system.

If the incident occurred on a first-party system, below are action items for plan fiduciaries:

- *Establish an incident response team*. Assemble a group of individuals who will be responsible for addressing the cyber incident in a timely manner.
- *Notify cyber liability insurer and review cyber liability insurance policy*. If drafted properly, cyber liability insurance generally will cover losses incurred by ERISA plan sponsors and fiduciaries, including corrective actions, investigations, and defending claims. It is important to understand what is covered by the policy, and what steps the policy requires the employer to take in order to recover under the policy. For example, employers should determine whether the policy mandates a third-party forensic investigation.
- *Conduct cyber forensic investigation.* A cyber forensic investigation should be conducted to preserve the digital evidence, perform digital forensics, and determine the affected parties, the scope of the incident, the records compromised, and the timeline of the incident. The cyber forensic team can determine if an attack is ongoing and firm up the employer's defenses to halt continuing damage. Most state breach notification laws require notifications to consumers and to state attorneys general to detail how the data breach occurred and the precise dates of unauthorized access to the system. While many employers have information technology (IT) professionals on hand, digital forensics is a highly-specialized skill set and a digital forensics team can help employers piece together any evidence and understand the scope of a breach. An independent third-party investigation is viewed more favorably by regulators, and internal IT teams would be significantly disrupted if their resources were devoted to the investigation.
- *Conduct a legal analysis to determine if the jurisdiction's data breach notification law has been triggered*. Requisite notification to the affected individuals, regulators, and enforcement authority vary depending on the jurisdiction and the scope of the incident. Also, consider the requisite timelines when determining notification obligations, as some states require notification to regulators as soon as 14 days following the discovery of the incident. Notice to the national consumer reporting agencies also may be required, if the total number of affected employees meets the threshold that triggers this obligation, depending on the jurisdiction and scope of the breach.
- *Draft notifications and internal messaging scripts, and communicate strategy with third-party administrator/call center*. The employer's executive and communications teams should be prepared on how to respond to tough questions and deliver messages to employees, and third-party vendors should have employer-approved scripted responses and frequently-asked questions available as soon as possible.
- *Determine mitigation strategy*. If the incident involves sensitive personally identifiable information such

as Social Security numbers or bank account information, provision of identity theft monitoring services to participants (and beneficiaries, where applicable) may be advisable. Depending on the nature of the information compromised, the plan sponsor may wish to extend the length of identity theft monitoring services for a period longer than required by law.
- *Develop strategy for permitting employees time to address/discuss issue*. For example, if affected employees work in a factory setting, permit employee breaks to call the plan's recordkeeper or to set up monitoring services.

If the incident occurred on a third-party system, below are action items for plan fiduciaries in addition to those listed above:

- *Examine contractual agreement with third-party vendor*. The provider may be responsible for conducting a forensic investigation and covering related costs, or for providing notifications to consumers and regulators and related costs.
- *Employer control of process*. The employer may want to take control of the notification process and messaging to confirm it is consistent with their branding and communication strategy.
- *Encourage outside legal counsel to interact with legal counsel for the third-party.* Outside counsel can help to identify any risks to the employer related to how the third-party may elect to message the event to affected parties and will be in a position to advise the employer on these risks. Outside counsel also may coordinate with the third-party's counsel for the purpose of instituting changes to notifications or coordinate a response to a regulatory inquiry.
- *Assess third-party liability and/or negligence.* Because of the implication of ERISA, participants will be able to pursue claims against the plan administrator and other fiduciaries to make them whole for their losses, but depending on the reason for the incident, the employer may want to pursue damages or indemnification for losses incurred. This underscores the importance of a thorough review of the service contract before an incident occurs.
- *Continue to monitor service provider throughout response*. Recall that ERISA imposes additional duties on fiduciaries to monitor service providers to the plan. Delegation of the services to another party does not absolve the plan sponsor of its duties to monitor the third-party and, if appropriate, remove or replace such vendors.

Develop Mitigation Plan

- *Assess gaps and improve security protocols to avoid similar incidents in the future.* Consider engaging a third-party vendor to conduct a cyber-risk assessment with a specific view towards the circumstances that enabled the incident to occur in the first place. Also, employers may want to revisit or re-negotiate service contracts in light of the incident, or consider a request for proposal for alternative vendors. For example, employers may consider requiring service providers to be proactive in communicating attempted breaches or theft incidents, rather than just communicating actual breaches, similar to the communication protocols required by many HIPAA business associate agreements for welfare plans. Improving documented processes and procedures for addressing a breach can help establish the employer's fiduciary prudence (and, correspondingly, reduce fiduciary exposure) in addressing cyber-related risk.
- *Revise or expand scope of cyber liability insurance policy*. In the event that certain losses were not covered by the policy, consider expanding the scope of coverage.
- *Update plan documentation and communications*. Consider including details in summary plan descriptions or other plan communications for what to do and who to contact in the event of a data breach.
- *Train employees*. If the incident occurred on a first-party system, train employees on common risk areas for a cyber-attack, examples of other types of breaches and how to prevent them, and how to follow security protocols adopted by the employer or its vendors.

As is the case with cybersecurity generally, potential cyber threats against retirement plans are becoming more commonplace and more complex each year. Congress is considering taking action to specifically address the unique responsibilities of ERISA plan sponsors and fiduciaries in the event of a breach. Until such guidance is issued, however, the existing legal framework governing responses to these types of threats can be difficult to maneuver, as it is a hodgepodge of fiduciary laws created without cybersecurity in mind, as well as state and federal laws that are not

directly tailored to the retirement plan sector. In light of this uncertainty, upon identification of a threat or incident, it is of the utmost importance for plan sponsors and fiduciaries to actively engage all stakeholders and legal counsel, document the steps taken, and improve the processes going forward. ■