Considerations for an Employee Benefit Plan Cybersecurity Policy

By Michelle Capezza and Christopher A. Lech

New York City Bar Association CLE Program
Cybersecurity Risks for Employee Benefit Plans
November 14, 2019

Fiduciaries of employee benefit plans, which are governed by the Employee Retirement Income Security Act, of 1974, as amended ("ERISA"), are held to a very high standard of care to ensure that the plan is operated and maintained in the best interest of plan participants and beneficiaries. The extent to which ERISA fiduciary responsibility applies to the protection of plan participant and beneficiary data and personally identifiable information is not clear under current law. With the ongoing advancements in technology (including with regard to the array of technological tools that have emerged to aid in the administration and delivery of employee benefits), and the novel cybersecurity risks that those advancements bring, there is widespread concern for the security of the employee data that is collected, transmitted, processed and stored with regard to employee benefit plans and for the security of the assets in participant accounts. To date, there are protocols and guidance for the privacy and security of protected health information but there are no clear protocols for ERISA plan fiduciaries to ensure the security of personally identifiable information, despite their equal vulnerability to data breaches.

In recent years, the ERISA Advisory Council has asked the Department of Labor to provide guidance on how plan sponsors should evaluate the cybersecurity risks they face with regard to plan data and personally identifiable information so that it can be properly managed, especially with regard to third party relationships for plan administration. Retirement industry groups such as the Spark Institute and the Financial Services Information Sharing and Analysis Center joined forces to establish the Retirement Industry Council to share information about new data security threats and strategies for improving security in the retirement market. The Spark Institute, through its Data Security

Oversight Board, also worked to develop standards for recordkeepers to demonstrate the security capabilities of their systems, including through reporting of their system controls.

Individual States continue to issue rules for handling of employee information and data in general, which raises ERISA preemption questions regarding their application to employee benefit plan administration. In February 2019, the U.S. Congress issued a written request to the U.S. Government Accountability Office to examine the cybersecurity of the private retirement system (the "Congressional Request Letter to GAO") noting that despite various initiatives and forums, "the cybersecurity safeguards, risks and liabilities for plan sponsors and participants remain ill-defined, especially with regard to major data breaches or advanced persistent threats."

In light of the foregoing, plan sponsors and fiduciaries must be cognizant of these developments and do their part to ensure that they have controls in place to prevent security breaches of plan participant data and assets, and that they have addressed these considerations with service providers. As noted in the Congressional Request Letter to GAO, current law does not address a number of questions related to cybersecurity and retirement plans fall within a patchwork of federal and state laws and regulations. While there is no clear fiduciary mandate under ERISA, plan fiduciaries do have a duty to carry out their responsibilities prudently and in the best interests of plan participants and beneficiaries. Employers that take the time to develop a benefit plan cybersecurity policy ("Policy") that addresses these issues in a thoughtful manner will be well-positioned to demonstrate prudence and diligence in these efforts, and prepared to act in the event of a data breach.

In light of the current landscape, and until laws and regulations establish clear and specific requirements, ERISA plan sponsors and fiduciaries should consider, at a minimum, taking the following actions, which are by no means exhaustive:

Assemble a qualified team. Given the complexities involved in understanding data systems and security controls, organizations must assemble a qualified team of individuals to ask the right questions, and review and interpret the answers. The team may include individuals from HR, IT, legal, compliance, risk management, and any

organizational cybersecurity leaders. The team should identify its areas of risk and define its protocols around data collection, transmittal, processing, storage, encryption, outsourcing, and breach notification and response. These developed protocols should then be properly executed and updated in compliance with applicable laws. Designated employee benefit plan fiduciaries should also provide input and incorporate organizational protocols in an approved Policy as part of its fiduciary best practices for benefit plan governance. If an organization does not have adequate in-house resources to develop a Policy, it should obtain qualified outside assistance.

Identify the data. Organizations must define the types of employee data that they are handling, and set parameters regarding its maintenance and security. Employee benefit plans store extensive amounts of personally identifiable information ("PII") for participants and beneficiaries, such as Social Security numbers, addresses, dates of birth, and financial information. Such information may be accessed by various personnel and service providers, which makes it vulnerable to data breaches. An initial step should focus on limiting the amount of information that is collected to categories that are absolutely crucial for the maintenance and administration of the plan. Further, depending on the type of benefit plan program, privacy and security may require vetting through different channels. For example, the use or disclosure of protected health information ("PHI") will need to comply with Health Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy and security policies (and electronic transmission of health information will need to comply with the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009). This can become further complicated when participants use health-tracking wearable tools, which interact with health plans—the plan may need a business associate agreement with cloud or storage providers receiving PHI. With a retirement investment advice tool, plan fiduciaries should undertake due diligence of the tool, and the provider's privacy and security measures to protect PII. Moreover, given the lack of uniform legal requirements in this area, plan sponsors and fiduciaries should be mindful of various state and local laws that may impact, among other things, the collection, storage, and transmittal of this PII, where the definition of PII can vary depending on the jurisdiction in which the plan is administered or the participant is

located. Accordingly, plan fiduciaries should be cognizant of the types of data that is collected from participants and beneficiaries and who has access to it, the types of data that is shared with outside plan service providers, ways to limit the amounts of data shared, and methods to protect the security of the data in different environments.

Train employees. Organizations must ensure that all personnel who have access to employee data are properly trained in safeguarding it, including securing the transmission of any data to third-party service providers. Individuals should be designated to respond to any benefits-related data breach and follow procedures for reporting breaches through the appropriate channels of the organization. Internal personnel handling this data must be properly vetted, and measures must be taken to protect against security breaches from within the company. Plan fiduciaries should address how they would handle a data breach and response in the Policy.

Develop additional standards for selecting and monitoring service providers. Plan fiduciaries should establish cybersecurity guidelines for engaging, monitoring, and renewing service providers, such as confirmation of their cybersecurity program and certifications, details regarding how they encrypt and protect data, their breach notification procedures, and a review of Service Organization Control or similar reports regarding their privacy and security controls, levels of insurance, and scope of their assumption of liabilities. Plan fiduciaries should develop a list of due diligence questions to ask service providers in connection with RFPs and contract renewals. It is also important for plan fiduciaries to understand whether the service provider utilizes agents or subcontractors to perform the services and the chain of security measures and indemnification. Procedures should be established for any IT security review of service provider systems, including requests for penetration tests to detect security risks. Data privacy and security, breach notification procedures, liability, and indemnification provisions should be addressed in service agreements in accordance with the standards of the organization's Policy. Plan fiduciaries should also request periodic updates from their service providers on the cybersecurity measures they follow and any of their new initiatives which should be further noted in meeting minutes. Plan sponsors and fiduciaries should also ensure

that they have an emergency response game-plan in place that meets standards under applicable law to communicate any data security breach to participants, beneficiaries and appropriate authorities.

Address data interactions. Plan fiduciaries should understand how data is accessed by participants and third parties, such as through online access or requests for retirement account distributions or transfers. If not already doing so, plan fiduciaries should request that the service provider utilize enhanced measures such as two- or even three-step authentication for participants to access to the information. Consider having the service providers generate and issue more complex usernames and passwords, as participants frequently use the same passwords and usernames across different websites. Also, consider setting up alerts for unusual behavior and educate employees on the steps they can take to protect their benefit plan information.

Review security of mobile apps. Many new mobile apps allow plan participants to check account balances, contributions, and investment changes; request loans or distributions; and receive alerts and educational information. Apps also track financial and physical wellness, and collect and convey such information to benefit plans. Despite their convenience, however, the use of mobile apps provides yet another opportunity for data breaches or the actual theft of assets and benefit payments. Plan fiduciaries should make sure that the Policy sets forth the protocols that should be followed when introducing apps into any benefits program.

Cybersecurity insurance. In addition to errors and omissions and fiduciary liability insurance policies, cybersecurity insurance has emerged in recent years and can offer various types of coverage, including coverage for certain disaster recovery and data breach response assistance that can be triggered by a benefit plan upon a security breach. It is important to assess existing insurance and liability coverages to ascertain how cybersecurity insurance can fit within employee benefit plan insurance needs. It is necessary to also evaluate any cybersecurity insurance to ensure that it does not carve

out and exclude the specific coverage that is desired and then make any appropriate adjustments.

ERISA Bond. With certain exceptions, ERISA plan fiduciaries and every person who handles plan funds or property must be bonded. A plan official is considered to handle funds whenever his or her duties or activities are such that there is a risk that the funds or other property could be lost in the event of fraud or dishonesty on the part of the person, acting either alone or in collusion with others (such as duties related to the receipt, safekeeping and disbursement of funds, and relationships which involve access to funds or other property or decision-making powers with respect to funds or property which can give rise to such risk of loss). The question arises whether ERISA bonds can or should be obtained at levels that would effectively protect against theft of plan assets by a plan fiduciary or person handling plan funds or property via a cyber-crime. The underlying terms of any ERISA bond must be reviewed closely for exclusions in this regard.

Deletion of Unnecessary Data. As previously mentioned, plan fiduciaries and sponsors should limit the amount of data that is collected to that which is absolutely necessary. A corollary to that step is the deletion of data that is no longer necessary or that is no longer required to be maintained by document retention laws. In general, plan records must be retained for at least six years after the filing of a report—e.g., an Annual Form 5500—created from those plan records. As for records necessary to determine a participant's or beneficiary's entitlement to plan benefits the records must be kept "as long as a possibility exists that they might be relevant to a determination of the benefit entitlements of a participant or beneficiary." The latter requirement does not provide a clear timeframe for document retention and record retention policies must be designed prudently considering the various requirements and statutes of limitations; nevertheless, once a reasonable amount of time has elapsed, the information can, at the very minimum, be securely archived, thus eliminating some of the risk associated with hosting that data on systems penetrable by hackers via the internet. That being said, electronic documents are not easily deleted and external service providers may also need to be consulted. For example, even when a document is dragged-and-dropped in the "Recycle-Bin" on a

desktop, that may not, in fact, delete that document off of the computer's hard-drive or the cloud-drive that is constantly backing up the data stored on the computer. In fact, simply dragging-and-dropping a document into the Recycle-Bin or hitting the delete button can leave meta-data that contains an individual's personal email address, IP addresses, or other sensitive information contained within that document. Furthermore, where plan records are maintained by third party service providers or recordkeepers, plan sponsors should ensure that service agreements address secure access to these records and proper transfer, retention and destruction of records following termination of services. Once again, consultations with legal and/or IT departments and advisors can aid in determining what information can be deleted, how such information can be properly deleted, and, if information cannot be deleted but can be archived, how such information can be safely stored.

Conclusion

The complexities of the issues concerning cybersecurity for employee benefit plans increases each day, and the law is evolving. Yet, the risks are tangible. Plan sponsors and fiduciaries cannot ignore the realities that these issues present. It is time for plan sponsors and fiduciaries to develop a prudent benefit plan cybersecurity policy that will enable them to face the challenges of participant and beneficiary data privacy protection head-on, and reduce potential losses and liabilities.