Cybersecurity and ERISA: Fiduciary Obligations to Safeguard Plan Participants' Data

ARIEL GAKNOKI

There have been numerous instances of high-profile cybercrime cases over the past couple of years spurring lively discussions in the ERISA community about the potential threat this type of crime poses to plan assets and personal data of plan participants and beneficiaries. Except when there has been a high profile cyberattack, news coverage of most incidents is minimal, even though the threats and occurrences of such attacks are significant. The largest ransomware attack in history took place recently, affecting tens of thousands of computers in nearly 100 countries. Those affected were required to pay a specified amount of money in order to take back possession of their own information, but the damage had already been done. Once information is shared and disseminated, it can never be fully re-possessed, nor can its privacy and security be fully re-established.

It is not a coincidence that the increasing pervasiveness of cybercrime parallels the upward trajectory of technological advancements in electronic data transferability, accessibility and storage. Electronic storage of plan data has been the industry standard for quite some time, but more complex and sophisticated forms of electronic storage, including cloud storage and remote server storage, have continued to evolve at a rapid pace. Furthermore, phone applications, remote employees, third-party administrators, and IT support are data access points that increase the potential for information to be infiltrated.

Although cybercrime is listed as one of the Federal Bureau of Investigation's top priorities, cybersecurity issues, in the context of maintaining privacy and security around employee benefit plans, remain largely unaddressed. The main concerns cyberattacks raise for employee benefit plans include the unauthorized collection of personal identity and personal identifiable information ("PII"); the theft of money from bank accounts, investment funds, and retirement accounts; and the infiltration of plan administration, service provider and broker systems. In February 2015, hackers breached Anthem, Inc.'s computer system and publicly released the personal information of an estimated 80 million customers and employees. In June 2016, more than 90 deferred-compensation retirement accounts of Chicago municipal employees were breached. In July 2016, a cyberattack targeted a grocery workers union pension plan in St. Louis. These significant threats of identity theft and loss of plan assets via hacking of plan financial data emphasize the importance of reviewing, identifying and overhauling the less than rigorous cybersecurity policies

and procedures most entities possessing PII have in place today. Cyberattack threats also warrant examination of the responsibilities of benefit plan fiduciaries with respect to cybersecurity.

Responsibilities of ERISA Fiduciaries

Under Section 404(a) of ERISA, a benefit plan's fiduciaries must discharge their duties to the plan solely in the interest of the participants and beneficiaries and for the exclusive purpose of providing for their benefits. These duties must be carried out with the care, skill, prudence and diligence under then-prevailing circumstances that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.[1] Because benefit data includes participants' names, Social Security numbers, account information and PII, it is increasingly important for ERISA plan fiduciaries to acknowledge and act on their inherent responsibilities to secure online plan data from cyberattacks. Failure to do so would almost certainly be counter to the prudence standard by which ERISA fiduciaries are required to abide.

Pursuant to Interpretive Bulletin 96-1 (the "Bulletin"), the selection and monitoring of a benefit plan's service providers is a key fiduciary responsibility, and plan fiduciaries assume liability for the failure to act prudently in selecting service providers.[2] While the Bulletin addresses the designation of a person(s) by plan fiduciaries to provide investment educational services or investment advice to plan participants and beneficiaries, the Bulletin has been interpreted more broadly to establish the requirement of prudence in service provider selections, including prudence in the selection of a service provider that maintains electronic plan data in order to keep that plan data private and secure. Accordingly, ERISA plan fiduciaries should consider cybersecurity when selecting service providers. Unfortunately, there is no direct guidance from the Department of Labor ("DOL") on cybersecurity considerations in carrying out this important process.

Developing Best Practices In the Absence of Cybersecurity-Related ERISA Regulation

The lag to adopt cybersecurity measures by ERISA fiduciaries is likely reflective, at least in part, of the lack of on-point guidance available to plan fiduciaries on *how* to meet their obligation to keep participants' and beneficiaries' information secure.

While there is currently no comprehensive federal law governing cybersecurity, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes privacy and security measures to protect the individually identifiable health information of participants in group health plans. Although data breaches have long been a concern of health benefit plan administrators under the HIPAA, these concerns about safeguarding PII are now being shared by fiduciaries of other types of plans, including pension plans, in the wake of an unprecedented number of breaches. Arguably, it is the fiduciaries of 401(k) and other benefit plans not subject to HIPAA's privacy and security measures whose responsibilities have expanded to include the implementation and management of processes minimizing cyber risks, since health benefit plans are already required to comply with those measures. A health plan fiduciary's compliance with ERISA requires compliance with HIPAA, and therefore a HIPAA breach via disclosure of PII to unauthorized individuals could trigger a breach of ERISA's prudence standard. However, HIPAA's privacy and

security requirements only require health plan sponsors to consider how potential breaches might occur and what measures should be implemented to avoid them. The mere consideration of how to protect PII is likely not enough to meet the broad fiduciary prudence standard under ERISA. As a result, data breaches and the fiduciary obligations associated with safeguarding against such breaches should be the concern of *all* plan fiduciaries equally, regardless of whether they are already subjected to HIPAA's privacy and security rules. Accordingly, it is increasingly important for any individual or entity interacting with a plan to be knowledgeable regarding the effect plan data and asset cyber breaches would have on participants and beneficiaries, as well as plan fiduciaries' duties under ERISA to implement defenses against cyber threats to PII.

The ERISA Advisory Council ("Council"), established to advise the Secretary of Labor, examined cybersecurity considerations as they relate to pension and welfare benefit plans in 2011 and re-visited the issue in 2016. The 2011 Council issued a report urging the DOL to issue guidance on the obligation of plan fiduciaries to protect the PII of plan participants and beneficiaries. The 2016 Council went further, intending its report to be a reference for plan sponsors to secure benefit plan data and assets from cybersecurity risks. To date, the DOL has not taken an official position regarding the role and responsibilities of plan fiduciaries in addressing and preventing cyber risks in response to the Council reports. As a result, and due to the increasing sophistication of cyber attacks, it is not advisable for plan fiduciaries to wait for guidance from the DOL before taking all prudent actions that are necessary to safeguard benefit plan data and assets.

Best Practices

Given the broad scope of an ERISA fiduciary's obligation to act with prudence, it is in the best interest of all parties involved with ERISA plans to begin developing systems and procedures for properly handling and securing PII. The ERISA Advisory Council recommendations may represent the foundation for future regulatory or statutory efforts to address plan fiduciaries' responsibility for cybersecurity matters. As such, the Council's proposed strategies should serve as a baseline for the standard of care ERISA fiduciaries should implement when addressing such matters.

Cybersecurity issues and concerns in employee benefit administration include breaches of the information systems used in the industry, the misuse of PII and benefits that are stored in those systems, and the impact of cyber threats on plan sponsors, service providers, participants and beneficiaries.[3] Guarding against cybersecurity breaches is a complex process, and involves instituting systems that not only detect and eliminate the source of the breach, but also measure the damage done, recover any data lost, and restore the integrity of the system.

The following are some affirmative actions plan fiduciaries can take to build a framework upon which they may base a cybersecurity risk management strategy:

- Consider purchasing cyberliability insurance;
- Perform due diligence of third-party service provider systems by vetting third-party administrators' ("TPAs") cybersecurity programs and formally requesting that TPAs provide information regarding their security systems and risks;
- Review and amend agreements with service providers to ensure there are contractual provisions mandating the protection of data and allocations of liability;

- Monitor third parties and employees with access to plan data; and
- Become more informed regarding the functionality of cloud computing and remote data storage processes to better understand where PII is located in the organization's systems and how it is stored or protected.

The above action list represents just a fraction of the procedures and policies that a plan fiduciary must consider to ensure a secure data system. The consequences of a data breach are severe and will be even more so for plan fiduciaries if their failure to address cybersecurity issues is determined to be a fiduciary breach. Regardless of whether it is explicitly stated by a governing authority, plan fiduciaries are under a fiduciary obligation to secure participant data under ERISA. The best practices listed above are ways in which a fiduciary may begin to address the threat that continues to evolve in this area and determine how to fulfill their obligation.

To prudently administer their plans, plan fiduciaries should not wait for formal guidance on these issues, but rather take action as soon as reasonably possible to develop effective practices and procedures for combatting data breaches that put PII at risk.

---

[1] 29 U.S.C. §1104 (2011) https://www.gpo.gov/fdsys/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap18-subchapI-subtitleB-part4-sec1104.htm

[2] Interpretive Bulletin 96–1; Participant Investment Education; Final Rule, Federal Register (1996), https://www.dol.gov/ebsa/regs/fedreg/final/96_14093.pdf (last visited Jun 12, 2017).

[3] *Id.*

JUNE 2017

EMAIL ARIEL GAKNOKI