2016 Advisory Council on Employee Welfare and Pension Benefit Plans

Cybersecurity Considerations for Benefit Plans

Issue Chair: Deborah Tully
Issue Vice-Chair: Jeff Stein, Deborah Smith
Drafting Team: Tazewell Hurst, Elizabeth Leight, Stacy Scapino, Christine Hwang

Description of Issue:

Cyber threats, including the risks of compromised data and assets, has become a daily headline, Individuals and institutions are continually exposed to cyber threats as information is increasingly exchanged in virtual environments across multiple intermediaries and more financial transactions move to a mobile, cloud-based environment. No individual, organization, or industry is immune from cyber threats, including benefit plans. The operation and administration of benefit plans requires the sharing of data and assets among multiple parties, including third party administrators, actuaries, auditors, and trustees, to name a few. It is critical for plan sponsors and vendors to manage this data with the objective of minimizing exposure to the cyber threats that exist now and will develop in the future.

Cyber risks cannot be eliminated but they can be managed. What can and should plans do to address and manage the risks? Plans vary widely in size and complexity, so one approach does not fit all. Most plans do not have unlimited resources to devote to administration. Using the fiduciary standard that plan assets are to be used only for paying benefits and the reasonable administrative costs of providing those benefits, how can a plan administrator assess what is a reasonable approach for cyber readiness relative to the plan's assets?

In 2011, the Council studied Privacy and Security Issues Affecting Employee Benefit Plans (other than health care plans). The 2011 Council report included, among other things, recommendations with respect to guidance and educational materials for plan sponsors, plan participants and vendors. Specifically, the 2011 Council recommended that the Department of Labor (1) provide guidance on the obligation of plan fiduciaries to secure and keep private the personal identifiable information ("PII") of participants and beneficiaries; and (2) develop educational materials and outreach efforts for plan sponsors, participants and beneficiaries to address issues of privacy and security of PII.

The 2015 Council devoted some of its time to looking at cybersecurity issues in the context of the two overriding topics covered by the Council. After an initial review and witness testimony in the May 2015 hearings, it was determined that the topic deserved more attention and should be taken up by a future Council in more depth.

The 2016 Council will complement the work of the 2011 and 2015 Councils by focusing specifically on outlining the scalable elements of cyber risk management strategies for benefit plans. The goal of the 2016 Council is to offer the Department of Labor draft materials that will help plan sponsors understand, evaluate and protect benefit plan data and assets from cybersecurity risks. While the 2011 Council focused solely on retirement plan privacy and security issues, the 2016 Council will examine the issues that may be common to retirement and health and welfare plans, especially in

light of the growing similarities and inter-relationships between the two types of plans, and the proliferation of asset based health care accounts such as health savings accounts.

Objective and Scope:

We are interested in learning about the elements of a scalable cyber risk management strategy for benefit plans.

The Council is examining this topic and intends to draft recommendations to the Secretary of Labor for consideration. Our study will include the following:

A. As background, review the general types of cybersecurity risks that benefit plans are exposed to and how the overall threat environment is evolving.

B. Obtain information about the steps, processes and controls that plans and third party providers are taking to address these risks.

C. Examine how cybersecurity risks and exposure differ between small plan sponsors and large plan sponsors, with the objective of tailoring guidance and education accordingly.

D. Draft materials that may help plan sponsors identify and establish a scalable cyber risk management strategy.

E. Draft materials that may help plan sponsors incorporate cybersecurity risk management in the vendor selection and monitoring process.

F. Invite interested parties to submit sample tip sheets, checklists and other educational tools that can be used to provide plan sponsors, vendors and plan participants with guidance on navigating cybersecurity risks related to their benefit plans.

The Council is aware of potential issues that may exist regarding whether cybersecurity is a fiduciary responsibility and whether existing state cybersecurity regulations are preempted by ERISA. The Council does not intend to address these issues within the scope of this study.