TRUCKER ✦ HUSS

U.S. Senate Committee Eyes Lack of Guidance on ERISA Cybersecurity

ROBERT R. GOWER and
FREEMAN L. LEVINRAD

APRIL, 2019

It seems that every day, a new high-profile data breach is in the news. With increased reliance on the internet to transmit personal information, the potential for breaches has grown significantly. Defined contribution plans, which now hold over $5 trillion in assets, are by no means immune from cyber-attacks. As the retirement industry works to utilize technology to enhance plan features, increase access to information, and provide for better participant control over savings and investment strategies, any vulnerabilities in electronic transmittal of information make attractive targets for cyber criminals. Social Security Numbers, birthdates, compensation, and direct deposit information are all subject to exposure. When a breach does occur, in addition to the risk of account theft, there may be significant costs associated with restoring security and the interruption to plan administration. With the retirement savings of participants at stake, plan sponsors should be considering steps they can take to protect their benefit plans.

There is no definitive answer to the question of whether the sponsor of a benefit plan is subject to the fiduciary standards of ERISA with respect to implementing cybersecurity measures to protect participants' financial data (in other words, whether a plan sponsor must act with the "care, skill, prudence and diligence under the circumstances then prevailing that a prudent [person] acting in like capacity and familiar with such matters would use" in such matters). Nevertheless, it seems that the prudent plan sponsor should act under the assumption that a court would apply the ERISA fiduciary standards in this context, especially given that participant financial data has actual market value: It can be bought and sold on the black market — and, moreover, if breached can be used by criminals to impersonate plan participants or beneficiaries and actually steal their plan assets. However, the actual steps and measures that a benefit plan sponsor should follow for cybersecurity are not always clear.

Acknowledging a complete lack of guidance, on February 12, 2019, the Senior Pensions Counsel for the Senate Committee on Health, Education, Labor, and Pensions sent a letter to the U.S. Government Accountability Office (GAO) requesting guidance from the GAO on issues related to cybersecurity and the private retirement system. This letter explains that although retirement plan fiduciaries are responsible for designing and administering plans in the best interests of plan participants, current law applicable to retirement plans doesn't address a number of questions related to cybersecurity. The letter requests that GAO address a list of ten important questions about cybersecurity and retirement plans. Most importantly, the letter asks to what extent existing federal laws and regulations require plan sponsors, recordkeepers, and other retirement plan service providers to protect plan data and plan participants from cybersecurity risks.

The letter to the GAO demonstrates that there are numerous unanswered questions regarding cybersecurity and the responsibilities of a benefit plan fiduciary with respect to protecting the data and assets of its participants from cyberattacks. In June 2017, we wrote about cybersecurity and certain best practices that retirement plan fiduciaries could follow given the current lack of guidance in this area. Since then, the importance of a strong cybersecurity strategy has only been reinforced as a result of high-profile breaches coming to light. Accordingly, it is worth revisiting and expanding on some best practices benefit plan fiduciaries should consider in order to protect their participants' financial data and plan benefits. Best practices include:

- Reviewing service providers' cybersecurity safeguards using audit reports under the standards established by the Spark Institute (these standards are described in detail in a whitepaper titled Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective);
- Ensuring that benefit plans are covered by cybersecurity insurance (note that many corporate general cybersecurity policies exclude benefit plans);
- Obtaining (and retaining) copies of service providers' information security policies and procedures, and understanding the contents of these documents. In so doing, plan sponsors should consider whether service providers should be subject to the plan sponsor's standard corporate information security policy, or, in turn, review service providers' information security policies for sufficiency. When negotiating service provider agreements, plan sponsors should consider including language as to a service provider's duties and liabilities — and the duties and liabilities of any subcontractors or agents of the service provider — with respect to implementing and following cybersecurity safeguards and notifying the plan sponsor of data breaches (similar to the business associate agreements that are required under HIPAA for health plans).
- Reviewing data transmittal policies and practices. Consider implementing policies that avoid sharing unnecessary participant data (for example, always using an employee identification number as opposed to a social security number in electronic transmittals), and ensure that all internal and/or third-party plan portals are secured.
- Developing procedures to respond to a breach should one occur, including communication strategies with participants, and practical steps that can be taken with service providers to mitigate the impacts of the breach and establish post-breach monitoring.

Having such procedures will help establish fiduciary prudence in responding to a breach.

If you have any questions, please contact the authors of this article or the attorney with whom you normally work.

EMAIL ROBERT GOWER