ERISA ADVISORY COUNCIL
CYBERSECURITY INSURANCE AND EMPLOYEE BENEFIT PLANS
JULY 19, 2022
TIMOTHY ROUSE

My name is Tim Rouse, and I am the Executive Director of the SPARK Institute. Thank you for inviting me to testify before the ERISA Advisory Council ("the Council") once again. The SPARK Institute ("SPARK") represents defined contribution plan recordkeepers, mutual fund companies, brokerage firms, insurance companies, banks, consultants, trade clearing firms, and investment managers. Collectively, our member firms administer the retirement plans for over 100 million American workers.

Particularly through the efforts of our Data Security Oversight Board ("DSOB"), the SPARK Institute has long sought to help recordkeepers eliminate the ever-growing cybersecurity and fraud threats that pose a risk to the financial security of retirement savers. In pursuit of this goal, the SPARK Institute's DSOB has developed: (1) Industry Best Practices for Data Security Reporting, which provide a standard framework for retirement plan recordkeepers to report their cybersecurity capabilities to plan sponsors; and (2) Industry Best Practices for Fraud Controls, which highlight a minimum set of fraud controls that should be considered by retirement plan recordkeepers and their plan sponsor clients.

These industry best practices have increased awareness about cybersecurity and fraud risks, standardized practices among retirement plan recordkeepers and other plan service providers, and helped to mitigate cybersecurity and fraud risks facing retirement plans and participants. While cybersecurity insurance is one component of an overall strategy for addressing cybersecurity threats, the SPARK Institute believes that cybersecurity threats are best addressed through proactive and preventive measures that reflect the industry best practices developed by the SPARK Institute's DSOB.

Given SPARK's longstanding commitment to these important issues, we were pleased to see that the Council is once again exploring employee benefit plan cybersecurity issues, with a current focus on the availability of, and features associated with, cybersecurity insurance that may be issued to plans. While some of the issues identified in the Council's Issue Statement are more properly suited for plan sponsors and property and casualty insurers,[1] through my testimony today, I would like to share the SPARK Institute's views on cybersecurity insurance from a recordkeeper perspective. Thus, my testimony reflects observations regarding the marketplace for cybersecurity insurance that is issued to retirement plan recordkeepers, as opposed to policies issued to individual plans. Although these recordkeeper policies are analytically distinct from the policies that are

[1] For questions regarding policies issued directly to plans, SPARK recommends that the Council reach out to The Institutes in Malvern, Pennsylvania to get the best insights on which insurers offer products in this space and to learn about the underwriting standards these insurers use for these policies.

issued directly to plans, in effect, a recordkeeper's cybersecurity insurance policy may be highly relevant to individual plans and their participants when cybersecurity incidents occur and cybersecurity policies are not purchased by, or are unavailable to, individual plan sponsors. In that case, a recordkeeper's cybersecurity insurance may be the only insurance impacting an affected plan and its participants.

Cybersecurity Insurance[2]

With regard to the current cybersecurity insurance marketplace, the SPARK Institute believes that there is a common misunderstanding about what cybersecurity insurance policies cover and what they do not cover in the context of retirement plans. This is an important distinction that I would like to highlight for the Council's consideration today.

The SPARK Institute understands that the following expenses are commonly covered by cybersecurity insurance policies:

1. Legal expenses
2. Information technology forensics
3. Negotiation and payment of a ransomware demand
4. Data restoration
5. Breach notification to consumers
6. Setting up a call center
7. Public relations expertise
8. Credit monitoring and identity restoration
9. Defending against consumer class action litigation and funding a potential settlement
10. Legal expenses, fines, and/or penalties incurred due to a regulatory investigation
11. Loss arising from security failures, third-party hacks, a failed software patch, or human error
12. Lost income from reputational harm
13. Replacement cost of technology equipment rendered useless by an attack ("bricking")

The SPARK Institute also understands, however, that certain expenses associated with cybersecurity incidents are often excluded by cybersecurity insurance policies. For example, cybersecurity insurance policies often exclude losses attributable to employee fraud, theft, or robbery. Thus, while cybersecurity insurance policies may help insureds recover some losses associated with cybersecurity incidents, they do not make insureds whole for all incidents involving information technology and data systems.

Furthermore, we understand that coverage for certain types of incidents have increasingly been limited to very large and highly sophisticated firms. This is especially true in the case of insurance coverage that is sought for ransomware attacks. We believe that there may be a reluctance by some insurers to issue coverage for these events because ransomware presents a new threat to both retirement plans and providers. Cybersecurity experts are seeing sophisticated and organized crime groups that know the coverage limits on cybersecurity insurance policies and ask for ransomware amounts at those limits. If a firm is attacked by ransomware, it is not simply a matter of installing

[2] As previously noted, the information discussed in this section is based on cybersecurity insurance policies that are issued to retirement plan recordkeepers.

backup files. A firm must first identify the source and degree of the infection. If a cyber infection is severe, the firm is likely to need to rebuild its operating systems and platforms. This process could take weeks or even months to complete.

With respect to cybersecurity insurance for ransomware attacks, we can also report that this is an issue where SPARK's recordkeeper members have increasingly seen more questions from plan sponsors about whether a recordkeeper has coverage and what type of coverage it has in the event of a ransomware attack.

Fraud Insurance

Closely related to the issue of cybersecurity, over the past five-years, the SPARK Institute's members have seen a significant increase in the number and types of fraud attempts that are directed towards retirement plan participant accounts. Our members have always dealt with and maintained policies to deter and prevent fraud. However, unlike traditional fraud attempts involving friends and family members of participants, recordkeepers have recently seen a substantial increase in the number of fraud attempts that are being conducted by bad actors who are unknown to the participants that are being targeted.

We wanted to raise this issue for the Council's attention because, for certain instances of fraud, we understand that it can be difficult for recordkeepers to find an insurer that is willing to issue meaningful coverage. Moreover, to the extent that coverage will actually be issued to cover losses associated with fraud, coverage can be prohibitively expensive. Accordingly, with regard to losses associated with fraud, many recordkeepers simply choose to self-insure.

* * * *

On behalf of the SPARK Institute, I want to thank the Council for seeking our input, and I am happy to take any questions.