The SPARK Institute, Inc.
SHAPING AMERICA'S RETIREMENT

June 7, 2021

Ali Khawar
Acting Assistant Secretary
U.S. Department of Labor
200 Constitution Avenue, NW
Washington, DC 20210

RE: TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBER SECURITY PRACTICES

Dear Acting Assistant Secretary Khawar:

The SPARK Institute and its members welcome and support your new cyber security guidance. We applaud all efforts to protect American workers and their savings from criminals and share with the Department of Labor (the Department) the goal of minimizing any loss to fraudsters. With that goal in mind, SPARK members continually work together to share and develop ideas to strengthen our cyber security systems against intruders. Further, we appreciate the dialogue and partnership the Department has provided us with in helping to improve the system for protecting cyber security and reduce attacks.

Specifically, we want to commend you on the following points addressed in the Department's new guidance:

1. **The Department's Online Security Tips**—It is extremely helpful to highlight the shared responsibility that record keepers, plan sponsors, financial advisors, and participants all have in protecting these critical savings accounts. Also, the inclusion of links to the FBI and CISA's cyber incident websites are welcome. For too long, victims of cyber security attacks have been unsure of where to turn and to whom to report these crimes.

2. **The Department's Tips for Hiring Service Providers**—This guidance aligns nicely with the standards SPARK and its Data Security Oversight Board developed, and it is helpful that these guidelines acknowledge what many always assumed—that cyber security is a natural part of a fiduciary's responsibility to oversee the plan's service providers. Both the Department's guidance and the SPARK standards are built on two key principles to better assist the plan sponsor in fulfilling this fiduciary duty:

    a. The consumer should be provided standard cyber security information that can be used to compare service providers. That is precisely the goal of the SPARK standards.

    b. Basic cyber security information should be validated by trusted independent third-party auditors to ensure the integrity of all information.

While we support the work developed by your team, we recommend additional guidance be considered on a few points. First, the Department suggests that the service contract should identify how quickly the fiduciary is notified of "any cyber incident or data breach." While we agree with the Department's recommendation that the plan sponsor is appropriately informed of data breaches, plan sponsors must understand what is meant by a "cyber incident" or "data breach" when entering into contracts with service providers. Due to the rise of manual and automated attacks (such as account take-overs, mass registrations, etc.), every system in the world is constantly experiencing some level of breach attempt. Most never rise to a level of severity that becomes meaningful to a consumer. Properly identifying the right level of severity which would necessitate a notification is critical for this process to work effectively. It would be difficult for either the Department or the industry to adequately define a "cyber incident" or "data breach." We believe this is something better left to the parties to work out in their contracts.

Secondly, while we agree that a plan fiduciary should discuss the level of protection, including cyber security insurance, that the service provider offers, it is also important that the plan sponsor understand that cyber security insurance is a nascent industry. Product coverage can be confusing and unclear. Without this understanding, both plan sponsors and participants may believe they are covered against certain losses, when in fact they are not. For example, no cyber security insurance would likely provide coverage in the case of a participant simply providing their credentials to a third party who commits fraud.

Also, the guidance mentions penetration tests results, which are a critical component of any cyber security program. However, it must be made clear to plan sponsors that the release of a penetration test is unacceptable because the results of these tests contain lists of possible vulnerabilities to the service provider's system. Rather, the plan sponsor could ask for and receive the following information regarding penetration tests:

1. Are Penetration Tests conducted? And what type of test?
2. How often are these tests performed?
3. Who performs these tests? And what are their qualifications?
4. Do you follow CVSS, OCOAS, or other industry standard scoring?
5. Did your testing identify any material vulnerabilities (critical or high)?
6. What is your remediation policy for fixing identified issues? And what is your success rate for meeting this remediation goal?

Industry Best Practice - Penetration Testing 4-2020 (sparkinstitute.org)

Since the release of your guidance, our members have received hundreds of inquiries from clients and prospects asking how this guidance should be applied to their plans. While we welcome these conversations and encourage plan sponsors to learn more about the effort and resources our members employ to protect plan data, we have accumulated a list of questions from plan sponsors that require more explanation from the Department. Four examples are:

1. There are several ways to interpret the recommendation for "prudent encryption to protect all sensitive information transmitted and at rest."

2. You also recommend that "[p]rocedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant." Record keepers receive information directly from participants, and not all of it is provided back to the employer. Some information is related only to the participant's account and not part of an employer's human resources record. Additionally, the sharing of some data may conflict with privacy laws.

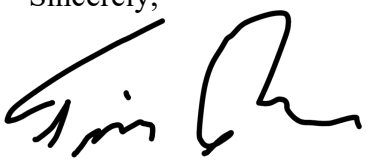
3. The document specifically recommends that "access privileges are reviewed at least every three months," but plan sponsors are inquiring whether risk-based quarterly reviews may be more appropriate, or whether that frequency is needed if other compensating controls are in place (e.g., automated access removals for terminations, transfers, etc.).

4. Will there be efforts to reconcile the DOL Cybersecurity Program Best Practices with the SPARK Data Security Reporting Best Practices?

We respectfully request a meeting with the appropriate members of your team to share these questions and discuss how to further educate plan sponsors. We believe that clarifying these points and other points will improve the dialogue between plan sponsors and their service providers, reduce confusion and better educate the consumer on these critical issues.

The SPARK Institute appreciates the opportunity to provide these comments to the Department. If you have any questions or would like more information regarding this issue, please contact me at (508) 838-1919 or Tim@sparkinstitute.org.

Sincerely,



Tim Rouse
Executive Director