SPARK INSTITUTE
SHAPING AMERICA'S RETIREMENT

WASHINGTON REGULATORY OUTLOOK

DOL Issues Cybersecurity Guidance for Retirement Plans

Michael Hadley
Partner
Davis & Harman LLP
Counsel, The SPARK Institute, Inc.

Adam McMahon
Associate
Davis & Harman LLP
Counsel, The SPARK Institute, Inc.

> The SPARK Institute has, for many years, facilitated the efforts of retirement plan recordkeepers to identify and share information regarding cybersecurity threats.

When asked in a recent interview about threats to the United States economy, Jerome Powell, the Chairman of the Federal Reserve, identified "cyber risk" as the threat that is most likely to cause a breakdown of our nation's financial system. This stark warning, as daunting as it may be, is unlikely to come as any surprise to the information security professionals who are actively combating cybersecurity threats directed at members of the SPARK Institute. Nevertheless, this succinct and straightforward assessment is a grim reminder of the cybersecurity risks that not only threaten the broader economy, but also the integrity of the retirement savings system that is facilitated by members of the SPARK Institute.

The cybersecurity threats facing retirement plans are, of course, not unique to the retirement savings system. After all, bad actors are not only launching attacks against 401(k) accounts, they are also attacking individual bank accounts, brokerage accounts, corporate information systems, and just about anything else connected to the internet. For retirement industry service providers that also offer non-retirement products and services, retirement plan assets and information only represent one piece of a larger cybersecurity puzzle.

At the same time, however, we also recognize that retirement plans are unique from a cybersecurity perspective. For example, because of automatic enrollment, there are many retirement accounts for which the owner has never taken any affirmative action. This means that these participants commonly do not register their accounts online, do not know how their assets are invested, and do not routinely check or manage their accounts.

In recognition of these unique needs, the SPARK Institute has, for many years, facilitated the efforts of retirement plan recordkeepers to identify and share information regarding cybersecurity threats. Furthermore, through the work of the SPARK Institute's Data Security Oversight Board, in 2017, SPARK produced a set of industry best practices ("SPARK's Best Practices") to help retirement plan recordkeepers communicate their full cybersecurity capabilities to retirement plan sponsors and consultants. SPARK's Best Practices set a baseline standard of 16 cybersecurity control objectives and recommend that plan sponsors obtain an independent third-party

audit of and report on these objectives. These efforts have not only helped service providers to better communicate with their clients, they have also promoted the use of strong cybersecurity protocols across the industry.

Outside of our industry's longstanding efforts to combat cybersecurity threats, on April 14, 2021, the Department of Labor ("DOL") released its own cybersecurity best practices for retirement plan recordkeepers, plan sponsors, and plan participants. DOL issued these best practices pursuant to its authority to interpret and enforce the Employee Retirement Income Security Act of 1974 ("ERISA"). Although ERISA does not include any provisions specifically addressing cybersecurity, its fiduciary responsibility provisions have generally been understood to make plan fiduciaries responsible for monitoring service providers. Until now, however, DOL had not provided any guidance on what that monitoring responsibility might mean with respect to cybersecurity threats.

In this Washington Regulatory Update, we will review DOL's recent cybersecurity guidance for retirement plans, discuss how this guidance is likely to impact the retirement industry, and discuss how policymakers in Washington are most likely to build upon DOL's latest efforts to combat the cybersecurity threats facing retirement plans.

Overview

DOL's recent cybersecurity guidance comes in three parts: (1) a set of cybersecurity best practices for plan fiduciaries and service providers; (2) a set of tips to help plan sponsors hire service providers with strong cybersecurity practices; and (3) a set of online security tips for retirement plan participants.

Cybersecurity Best Practices. DOL's best practices for plan fiduciaries and service providers generally revolve around the creation and maintenance of a well-documented cybersecurity program that is managed by senior executives, annual third-party audits, and annual risk assessments to update any cybersecurity program. These best practices generally do not identify specific technical standards. Instead, they identify the general policies and procedures that should be included in a prudently designed cybersecurity program. The SPARK Institute is pleased to see that many of the policies and procedures described in DOL's guidance overlap with SPARK's Best Practices.

Tips for Plan Sponsors. DOL's tips for plan sponsors are intended to help plan sponsors evaluate the cybersecurity practices of their plans' service providers. Among other tips, DOL recommends that plan sponsors ask their service providers about their cybersecurity policies and audit results, and compare those policies and results against industry standards adopted by other financial institutions. DOL's guidance also recommends that plan sponsors look for service providers that use a third-party auditor to review and validate cybersecurity, which is again consistent with SPARK's Best Practices. Plan sponsors are also encouraged to consider the service provider's track record based on public information and asking the service provider about past cybersecurity incidents.

Tips for Plan Participants. DOL's tips for retirement plan participants are intended to help reduce the risk of fraud and loss to participant accounts. DOL's tips include, for example, recommendations for participants to register their retirement accounts online, use strong passwords, keep software up to date, and avoid using free public wi-fi.

"The SPARK Institute is pleased to see that many of the policies and procedures described in DOL's guidance overlap with SPARK's Best Practices."

Key Takeaways

In the months preceding its release, DOL officials had been previewing the framework of their cybersecurity guidance with interested stakeholders. For example, during a cybersecurity event organized by the SPARK Institute last October, a senior DOL official announced that DOL would be issuing cybersecurity best practices, and its guidance would concentrate on a plan sponsor's selection of its service providers and the cybersecurity programs of those service providers. In this regard, much of DOL's cybersecurity guidance was expected.

However, notwithstanding the general consistency between what was expected and what was delivered by DOL in April, DOL's best practices addressed two issues that stood out to us as being particularly noteworthy: (1) DOL's express recognition of cybersecurity mitigation as a fiduciary responsibility; and (2) DOL's discussion of specific cybersecurity provisions that should be included in service provider contracts.

Fiduciary Responsibility. DOL's cybersecurity guidance expressly states that "[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risk." Although many industry stakeholders have interpreted ERISA's fiduciary provisions to include this obligation, DOL had not previously released guidance definitively placing cybersecurity mitigation within the scope of ERISA's fiduciary responsibilities. DOL's pronouncement is also consistent with a recommendation included in a recently released Government Accountability Office ("GAO") report examining cybersecurity risks faced by retirement plans.

Service Provider Contracts. In addition to DOL's general tips to help plan sponsors evaluate their service providers, DOL's recent guidance includes a discussion of specific cybersecurity contract terms that plan sponsors should seek to obtain in their service provider contracts. According to these contract terms, service providers would be contractually required to: (1) comply with cybersecurity and information security standards; (2) obtain third-party audits; (3) keep private information private; (4) prevent unauthorized uses and disclosures of confidential information; (5) meet a strong standard of care to protect confidential information against unauthorized access, loss, disclosure, modification, or misuse; (6) identify breach-notification standards; (7) cooperate with any efforts to investigate and reasonably address the causes of breaches; and (8) specify the service provider's obligations to meet all federal, state, and local rules pertaining to the privacy,

confidentiality, and security of participants' personal information. As part of this discussion, DOL also suggests that plan sponsors consider requiring their service providers to obtain cyber liability and privacy breach insurance.

Preliminary Reactions

In initial discussions with SPARK members, we have heard that most of the guidance came as no surprise, and our members, which are the most sophisticated providers in the industry, are up to the task of meeting DOL's expectations. We applaud DOL's work on this issue and will continue to engage with them. A few items did, however, stick out to us:

- **Fraud Versus Cybersecurity.** Much of the guidance relates to general cyber breach risks. And those risks are significant. But day to day, a much bigger risk to participant accounts is simply participants allowing criminals to gain access to their accounts. While providers can help mitigate this risk, participants ultimately need to be part of the solution. We were glad to see DOL publish guidance to help educate participants about their shared responsibility.
- **Disclosure of Breaches.** DOL's guidance suggests plan sponsors should be notified of any cyber incident or security breach. In the real world, however, systems are under constant attack, and there is no universally accepted definition of a cyber "incident." Suffice it to say that plan sponsors generally do not want to be notified of every incident.
- **Cyber Insurance.** DOL's guidance suggests plan sponsors should ask about cyber insurance and privacy breach insurance. This is a new and evolving product, and there are very few carriers willing to issue policies with complete coverage. There may simply not be policies available that provide the kind of coverage DOL contemplates.

Impact

DOL's cybersecurity guidance is generally framed as "tips" and "best practices." Accordingly, by its terms, DOL's guidance does not prescribe any minimum standards that must be followed and does not offer any safe harbor protections for plan fiduciaries and service providers that follow its directions. Nevertheless, we anticipate that DOL's cybersecurity tips and best practices will immediately have a direct impact on the retirement industry in the following ways:

- **Increased DOL Enforcement.** We understand that DOL's recent guidance is also being accompanied by increased DOL audit and enforcement activity regarding retirement plan cybersecurity, especially in the case of larger plans. This means that DOL audits will devote greater attention to cybersecurity issues and, similar to DOL's recent enforcement activity regarding missing participants, this activity will likely raise the profile of retirement plan cybersecurity issues more broadly.
- **Greater Scrutiny from Plan Sponsors.** DOL's tips and best practices will affect how plan sponsors and consultants evaluate service providers and how they document their selection process. Now that DOL has publicly announced its tips and best practices, there are heightened enforcement and litigation risks for plans and service providers that do not follow these guidelines.
- **Contract Negotiations.** To the extent that such terms are not already included, we expect that plan sponsors will insist that service agreements include the cybersecurity provisions discussed in DOL's best practices. Although DOL generally frames these provisions in the context of "tips" and "best practices," DOL's recent guidance indicates that service provider contracts "should" include these terms.

Outlook

By expressly stating that ERISA requires retirement plan fiduciaries to mitigate cybersecurity risks, DOL has sent a clear message that it believes it is responsible for overseeing retirement plan cybersecurity and that it intends to make cybersecurity a priority. Based on this expansive view of its statutory authority, we expect that DOL will seek to issue additional cybersecurity guidance in the coming years. This is especially true if DOL's increased audit activity uncovers gaps or weaknesses in existing cybersecurity protocols. Similar to its recently released best practices, future regulatory action could include additional guidance on cybersecurity programs and service provider contracts. For example, DOL could mandate cybersecurity disclosures by service providers, prescribe minimum security standards, or require specific contract terms.

Beyond these traditional security issues, DOL could also choose to weigh in on a related issue dealing with the question of whether information and data collected from retirement plans is considered a "plan asset" under ERISA. Such an effort would extend beyond traditional cybersecurity matters into questions about how plans are permitted to use plan and participant data, even when such uses do not increase the risks of fraud or unauthorized access to plan accounts. Although these issues have been unsuccessfully raised by plaintiffs in recent litigation against plans and service providers, DOL has yet to weigh in with its own views on the issue.

In addition to any future activity by DOL, Congress may also be eyeing its own cybersecurity standards, although we do not expect any legislative proposals to be become law in the near term. In 2019, the Chairwoman of the Senate committee with jurisdiction over ERISA, Patty Murray (D-WA), and the Chairman of the House committee with jurisdiction over ERISA, Bobby Scott (D-VA), requested GAO to examine the cybersecurity of the private retirement system. In March, shortly before DOL released its guidance, GAO published that report but did not recommend that Congress pass any legislation. It is possible that GAO will continue to focus on this issue and release additional reports. There have also been various federal cybersecurity and privacy proposals unveiled in Congress, although no bills have emerged at the moment as having sufficient bipartisan support for enactment.