The DOL Comes Out Swinging Against Potential Cybersecurity Breaches . . . and So Should the Plan Sponsor

*Brian Costello, AIF®, CPFA®**

Department of Labor (DOL) guidance, long awaited and perhaps years late, provides another enforcement tool for the DOL while practitioners seem to be noticing the lack of "how" guidance along with the emphasis on the "or else" stance of the agency. From an Investment Advisor standpoint, however, it allows another opportunity for conversations with clients and potential clients about how critical data security is to the entire system. Despite the overwhelming boom in real estate, retirement plans (in all forms) continue to be the locale for the vast majority of American wealth, which is at risk as ransomware attacks explode throughout the globe.

Timothy Hauser, deputy assistant secretary for program operations for the Employee Benefits Security Administration (EBSA) in the DOL, recently spoke at a conference sponsored by the American Institute of CPAs and the Association of International Certified Professional Accountants. The meeting took place around the time new rules were announced regarding protection of plan sponsors and participants from cybersecurity breaches. Long awaited and perhaps years late, the rules provide another enforcement tool for DOL while practitioners seem to be noticing the lack of "how" guidance along with the emphasis on the "or else" stance of the agency.

From an Investment Advisor standpoint, however, it allows us to reiterate yet again to clients and potential clients how critical data security is to the entire system. Despite the overwhelming boom in real estate, retirement plans (in all forms) continue to be the locale for the vast majority of American wealth. We unfortunately have a new problematic example: Scripps Healthcare located in California was the target of ransomware in April with the attack continuing well into May. The inability of that system and its patients to access critical private health care information, including but not limited to appointments, patient history, and the like, led to panic on the parts of both patients and practitioners. Everything from routine office visits to lab work to surgeries were postponed as the system had to reboot itself outside its intranet.

That example could translate easily to self-directed retirement plans. It is not difficult to imagine the havoc a ransomware attack could have on a plan, to wit: retirement payments not being made, partici-

**BRIAN COSTELLO* has over 30 years of investment experience and has successfully guided all aspects of retirement plans while building and maintaining relationships with clients to help them improve their employee benefits. As Chief Executive Officer of The Waterford Group, an Alera Group Company in Rochester, NY, Mr. Costello helps utilize his team's talents and skills to assist retirement plan sponsors in reaching their retirement plan goals. Mr. Costello holds the Accredited Investment Fiduciary® designation, the Certified Plan Fiduciary Advisor (CPFA®) credential and in 2019 was named a "Financial Times 401 Top Financial Adviser."

pants unable to change investments, new employees unable to start deferring, records becoming inaccessible to sponsors and third-party administrators . . . just a complete hard stop in all of the normal functions we take for granted. Add in an inopportune drop in the equity markets while participants are locked out of their accounts, and one can feel plaintiffs' lawyers easily gathering up large class action suits that make the current round of cases against colleges and universities seem trivial.

With that as background, Mr. Hauser took the microphone to emphasize that the DOL has shifted at least part of its focus to cybersecurity for employee benefit plans. When addressing cybersecurity, Mr. Hauser said that, "Plans hold lots and lots of money, and with lots of money there's lots of temptations for bad actors. . . . Similarly there's lots of personal information, confidential information, on plan systems. . . . So far, I think we've been fairly lucky in the plan universe. We have not had a huge catastrophic loss yet. But I do fear that that may just be a matter of time."

With that, the door was publicly opened to the information that the DOL will be auditing retirement plans for cybersecurity. Thus, after a period of what seems for most to be audit dormancy, questions will be raised "about basic computer hygiene and IT systems maintenance." In what we suggest caused eyes to roll, he added that those responsible for plan administration should be "paying attention" to whether their systems are secure. He added that plan sponsors also must pay attention to basic principles to ensure that administrators are taking appropriate steps for information technology security.

In the words of many, "ya think?"

In what seemed decades late, he added that plan fiduciaries should ask service providers if they follow best practices, and pay attention to whether contracts with service providers limit liability. Without apologies for being critical, in 2021 this is the advice that the DOL is providing?

Of course, the DOL's responsibility for patrolling the administration of Employee Retirement Income Security Act of 1974 (ERISA) plans runs deep, beyond retirement plans to millions of health care plans. ERISA requires all fiduciaries to mitigate risks, and in at least the past two decades and in fact longer, it is clear to us that it is not markets that could do the most damage but rather cyber criminals. A review of the guidance the DOL issued in April is appropriate here before we turn to what we at Waterford have insisted upon to keep our clients and their participants as safe as possible.

First, understand that the guidance from the DOL was labeled "informal," meaning it does not actually rise to a standard of providing a set of auditable rules. Rather, it issued informal guidance in three areas: "Tips for Hiring a Service Provider with Strong Cybersecurity Practices," "DOL's Cybersecurity Program Best Practices," and "Online Security Tips" responsible for plan-related information technology (IT) systems and data.

First, in its "Tips" provisions, the DOL appropriately pointed out that many if not most plan fiduciaries rely upon third-party service providers to perform tasks necessary to establish and maintain compliant benefit plans . . . like Waterford as an Investment Advisor, that in turns brings appropriate administrators to the table after significant due diligence and scrutiny. Under ERISA, plan fiduciaries must, among other actions, prudently select and monitor plan service providers. When engaging new service providers or monitoring existing service providers, most plan fiduciaries conduct a request for proposal (RFP). With

that in mind, the DOL cybersecurity guidance provides numerous recommendations for a plan's hiring a service provider as well as provisions for inclusion in the plan's service provider contract; we welcome the DOL shouting this from the mountaintop. Accordingly, among other important requirements and obligations, a fiduciary should also include, in the RFP, cybersecurity questions and representations to which a service provider must respond to be considered for the engagement. Along with a recommendation of specific terms to include in the service provider agreement that are intended to enhance cybersecurity (such as information-security reporting and notification requirements for cybersecurity breaches), the guidance set forth primary considerations for plan fiduciaries' evaluation of a service provider:

1. Consider the service provider's cybersecurity standards, practices, policies, and results; and compare these to standards adopted by other service providers.
2. Request validation of the service provider's cybersecurity practices and the levels of security standards that the provider claimed to have met and implemented.
3. Consider the service provider's industry track record (including prior security incidents and related legal proceedings).
4. Evaluate whether the service provider has experienced prior security breaches and how it has responded.
5. Consider the service provider's cybersecurity insurance liability coverage (including coverage for breaches caused by both internal and external threats).
6. Ensure, when contracting with a service provider, that the contract stipulates the provider's adherence to ongoing cybersecurity and information security standards.

In its "Best Practices" section, the DOL provides a checklist for recordkeepers and other service providers responsible for retirement plan data, recommending that plan service providers responsible for plan-related IT systems and data maintain:

1. A formal, well-documented cybersecurity program;
2. Prudent, annual risk assessments;
3. Reliable, annual third-party audit of security controls;
4. Clearly defined and assigned information security roles;
5. Strong access to control procedures;
6. Appropriate security reviews and independent security assessments for assets or data stored in the cloud or managed by a third-party service provider;
7. Periodic cybersecurity awareness training;
8. A secure system development life cycle (SDLC) program;
9. An effective business resiliency program addressing business continuity, disaster recovery, and incident response;
10. Encryption of sensitive data, stored and in transit;
11. Strong technical controls consistent with best security practices; and
12. A paradigm for appropriate response to any past cybersecurity incidents.

The third set, "Online Secu-

rity Tips," provides basic rules aimed at reducing the risk of fraud to plan participants and beneficiaries who review their retirement accounts online. Acknowledging that plan participants play a critical role in mitigating the risk, the tips seek to diminish the likelihood of retirement plan account losses caused by cybersecurity fraud. The DOL suggested these basic rules:

1. Routine monitoring of online retirement plan account(s);
2. Use of unique passwords for online accounts;
3. Use of multi-factor authentication;
4. Maintenance of updated personal contact information;
5. Closing of unused online accounts;
6. Avoidance of free wi-fi;
7. Avoidance of phishing attacks;
8. Use and maintenance of antivirus software; and
9. Immediate reporting of identity thefts and cybersecurity incidents.

Again, it should be noted that this guidance does not have the authority of a regulation, yet it sends a clear message to fiduciaries of what should be considered appropriate standards. The multifaceted approach, utilizing multiple parties, provides safety, but is lacking guidance whether ERISA preempts state cybersecurity laws. Of course, fidelity bond and fiduciary and other insurance needs should be reviewed to include the application of potential cyber breaches.

It should be noted that EBSA's Acting Assistant Secretary Ali Khawar told the ERISA Advisory Council this cybersecurity guidance is "just the beginning from an interpretive standpoint." The council was then tasked with investigating plan sponsor insurance options to protect against third parties who misuse plan participant data. Again, if a plan sponsor has neglected to previously do so, it is indicative of a much larger problem that we believe is the thought that delegation of duties by the sponsor is being equated to getting all responsibility and work out the door. We all know that is far from the truth, with hope that continued pressuring and education of plan sponsors will lead to them welcoming more responsibility, which equals better plans and happier employees.

Selling data—part of the problem? "Financial wellness" programs are part of a new value-added service for employees that emerging litigation and calls for regulatory oversight are catching up to a retirement industry that increasingly relies on participant data to market financial wellness programs. Especially during and after what thus far has been the height of novel coronavirus (COVID-19) issues, employers were eager to complement retirement planning and investment help with more basic tools, such as emergency savings and household budgeting in the midst of layoffs, furloughs, and significant fear of the future. It is not clear whether retirement plan service providers or plan sponsors came to this idea first (although we suspect with a fair amount of certainty that it was folks in our industry looking to help plan sponsors while keeping their brand front and center). This was not a bad thing on its face because clearly it is our industry that has access to employee data as well as to the employees themselves. Therein, however, lies the potential and perhaps realized problem.

Specifically, a number of lawsuits contend that providers are selling participant data to do a number of less-than-stellar things, primarily to sell financial products. Unfortunately, the access to data has

translated to pitches for high-interest credit cards or life insurance products (whether discussed as savings vehicles or not). Plaintiffs' lawyers have perhaps appropriately convinced employees that their employers are breaching a fiduciary duty to avoid conflict-of-interest transactions at the same time that the still-new government administration is bound and determined to tighten the rules governing fiduciaries (including issuing the above cybersecurity guidelines).

As an Investment Advisor focused on plan investments, we can readily admit we were taken aback to review the complaints in these cases. As a lead-up, it is not surprising that the cases focus on classifying identifying information and investment preferences for participants in participant-directed plans. The contention that this data is a "plan asset" in the same manner as the investments in the plan is both creative and smart, as it brings the fiduciary obligation immediately to appropriate monitoring and shepherding data and employees. Simply put, it must then necessarily include the duty to monitor who has access to this "asset" and how it is utilized. Well done, and we wholeheartedly agree! Not as a way to hurt plan sponsors, but rather as an appropriate method to have these corporations understand that the data is as precious as the funds.

Although a federal court has yet to find credence in the data as plan asset theory, that does not mean that attempts will stop to pierce the fiduciary veil creatively. We know that of the at least 22 class actions against universities for fiduciary failures, at least four of them have resulted in settlements where the prohibition against the use of data for cross-selling purposes is forbidden unless the participants ask about other financial products a firm sells.

The landscape seems paved by the courts to allow salespeople to sell financial products outside the traditional plans. We have never had that kind of "side gig" and never will, because we believe it to be a conflict of interest and unfair to participants. With the courts essentially blessing the idea, it is likely we will see more and more of this type of action.

And with good reason. An April PricewaterhouseCoopers survey found that more than *87% of employees* want help with their personal finances. That is an astounding percentage for agreement on any issue in this day and time, especially when it comes to financial issues. Note that the survey said that COVID-19 drove a full three-quarters of workers to seek jobs that offer additional financial benefits.

There is a lot to think about regarding cybersecurity, and even more to ponder when placed in perspective along other issues. With more guidance ahead, and ransomware becoming a bigger problem with every new incident, either the courts or public opinion (or perhaps even the DOL) will cause the change necessary for plans' protections to get up to speed.