VOL. 31, NO. 1 SPRING 2018

BENEFITS LAW JOURNAL

Cybersecurity and Employee Benefit Plans: What Prudent Steps Should a Fiduciary Take?

Amy Gordon, Joseph Adams, and Sheryl Falk

Many issues keep fiduciaries of employee benefit plans awake at night, but cybersecurity is especially troubling for many reasons. Employee benefit plans face significant cybersecurity threats and, given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating. Further, a plan fiduciary can have the best cybersecurity procedures in place, and yet the plan or a plan participant can still experience a cyber breach because of the numerous interfaces. Specifically, retirement plans, 401(k) plans, and 403(b) plans are typically administered by numerous parties. In addition to the plan sponsor, there is typically a trustee and a plan administrator (recordkeeper). Health and welfare plans have insurers or third-party administrators, a custodian or

Amy Gordon is a Partner at Winston & Strawn LLP, based in the Chicago office. She regularly advises clients on their self-funded and insured health plans, wellness programs, and onsite clinics. She also handles fiduciary issues and represents clients before the Employee Benefits Security Administration. Joseph Adams, also a Partner in the Chicago office of Winston & Strawn LLP, advises clients regarding executive compensation and employee benefits programs. Sheryl Falk is co-leader of Winston & Strawn's Global Privacy and Data Security Task Force. She concentrates her practice in data security, cyber and other internal investigations, trade secret litigation, and complex commercial litigation. She is a Partner based at the firm's Houston office.

trustee (sometimes), and the plan sponsor. Participants can log into benefit portals through their home, phone, and/or work computers.

These numerous interfaces each provide potential entryways for cybercriminals. A diligent plan fiduciary may wonder what it can do to prevent such a cyber breach. There are numerous non-profit, industry sector, and government resources that can assist a fiduciary in understanding best practices in securing employee benefit plan data.

PRIVATE AND NOT-FOR-PROFIT CYBERSECURITY ORGANIZATIONS

Significant cybersecurity efforts have been, and continue to be, developed to help organizations manage and navigate cyberrisk—generally, albeit not necessarily solely, with respect to benefit plans. For example, a not-for-profit consortium known as HITRUST was founded in 2007 to represent various providers in the healthcare industry, such as pharmacies, pharmacy benefit managers, and various manufacturers with regard to cybersecurity and raise the level of security within the industry. HITRUST developed a Common Security Framework (CSF), tools and cyber-risk Management Framework (RMF). The CSF in combination with the HITRUST Assurance program comprises the RMF. The HITRUST Assurance program provides a mechanism for accurate and consistent cybersecurity program evaluation and reporting. The CSF and Assurance program focus on data security, integrity, and privacy.

The American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee has formed a Cybersecurity Working Group to work in collaboration with the Auditing Standards Board to develop a consistent, profession-wide approach to performing and reporting on attestation engagements related to cybersecurity. The AICPA recognizes the HITRUST CSF as acceptable criteria and established guidance for Service Organization Control (SOC) reporting.

The SPARK Institute is a private-sector initiative that is working on establishing uniform data management standards for the defined contribution retirement plan market. SPARK has established a Data Security Oversight Board (DSOB) that oversees program development and implementation. The DSOB includes representatives from plan administrators, consultants, SPARK staff, and the Department of Homeland Security.

In addition, financial firms in the U.S. plan to expand a secretive project protecting bank accounts against crippling cyber-attacks so that it will also guard trillions of dollars in investment funds. The industry-led project, called Sheltered Harbor, already is looking to

expand its protections to 401(k) accounts and pension funds, whose breach could devastate the global markets.

GOVERNMENT EFFORTS REGARDING CYBERSECURITY

Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act) to encourage the use of anti-terrorism products, services, and technologies in civilian settings. The SAFETY Act specifically provides risk-management protections to firms that develop, sell, or deploy these technologies, as well as contractors, subcontractors, and consumers downstream. The SAFETY Act protections include liability limitations for "claims arising out of, relating to, or resulting from an act of terrorism" where Qualified Anti-Terrorism Technologies (QATTs) have been deployed. Although the definition of an "act of terrorism"—which triggers SAFETY Act protections—may not have originally contemplated financial harm arising from a cybersecurity attack within a benefit plan, an argument can be made that when a certain technology (product or service) is intended to protect critical infrastructure, and that technology has received a SAFETY Act "Designation" or "Certification," these protections may be applicable in the benefit plan context.

On February 12, 2013, President Obama issued an Executive Order called "Improving Critical Infrastructure Cybersecurity." This established U.S. policy to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The Cybersecurity Framework was developed and published one year later, on February 12, 2014, through collaboration of the government *via* the National Institute of Standards and Technology.[1]

U.S. DEPARTMENT OF LABOR'S ADVISORY GROUP

The ERISA Advisory Council (the Council), was established under Section 512 of the Employee Retirement Income Security Act (ERISA). The duties of the Council are to advise the Secretary of the U.S. Department of Labor and submit recommendations regarding the Secretary's functions under ERISA. In November 2011, the Council provided the Secretary a report titled *Privacy and Security Issues Affecting Employee Benefit Plans*.[2] In November 2016, the Council provided the Secretary another report titled *Cybersecurity Considerations for Benefit Plans*.[3]

In both the 2011and 2016 reports, the Council examined cybersecurity considerations as they relate to pension and welfare benefit plans. Both reports note, "There continues to be no comprehensive federal law governing cybersecurity for benefit plan service providers. There are laws that govern the financial industry's use of financial information, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act. These laws, however, do not apply directly to benefit plans or the sensitive individual data held in conjunction with those plans."

The Council focused on information that would be useful to plan sponsors, fiduciaries, and their service providers in evaluating and developing a cybersecurity program for their benefit plans. The Council also created materials for plan sponsors and fiduciaries to use when developing a cybersecurity strategy and program. Several witnesses that were interviewed for the 2016 report commented that there is no such thing as a cyberrisk elimination strategy. The Council recommended that plan sponsors and providers should approach cyberrisk management strategies with the understanding that a good program will not *eliminate* risks but rather *manage* them.

PRUDENT STEPS ERISA FIDUCIARIES SHOULD TAKE TO ADDRESS CYBERSECURITY

To educate and assist plan sponsors in their compliance efforts, the Council created the Cybersecurity Considerations Document. Although prevention of a cybersecurity threat is impossible, there are steps that can be taken to limit the threat. Every plan is different, and cybersecurity risk management is not a "one-size-fits-all" approach. Plan sponsors, administrators, fiduciaries, and other service providers must determine what is reasonable from a commercial perspective and an ERISA perspective for each plan. The cybersecurity risk management strategy cannot be a static checklist. Instead, the program should include regular reporting, frequent reviews, and process updates that are specifically tailored to the plans' needs. Suggestions for compliance include the following:

- Inventory the plan's data, and consider using, sharing, and maintaining only the minimum amount of data necessary. This applies to the plan sponsor's data, as well as that used, shared, and maintained by service providers.

- Devise a framework upon which to base a cybersecurity risk management strategy (*e.g.*, the NIST framework or the SAFETY Act as models or possible starting points).

- Establish a process that includes implementation, monitoring, testing and updating, reporting, training, controlling access, data retention and destruction, and third-party risk management.

- Balance the scope and cost of a cyberrisk management strategy against the size and sophistication of the plans and the plan sponsor.

- Decide what if any portion of the cyberrisk management costs should be borne by the plan versus the plan sponsor, including insurance.

- Ensure that any program also addresses any state-specific cyberrisk requirements.

- Review applicable contract provisions with service providers, and require vendors to attest that the service provider or vendor has proper procedures in place to protect the plan's data. Plan sponsors should monitor the cyber protocols and practices of these providers on an ongoing basis to ensure they are robust enough. Plan sponsors, fiduciaries, and third-party service providers may want to consider whether SAFETY Act certifications could fit into their overall cybersecurity risk management strategy. Plan sponsors can take advantage of the Act's liability protections by retaining vendors that have or use SAFETY Act-approved processes or procedures. Doing so may help protect plans from third-party liability for losses resulting from cyberattacks and can potentially provide further assurance around a third-party's cybersecurity processes and controls.

- Plan sponsors should evaluate their insurance coverage and bonding policies to ensure they are covered in the case of a cybersecurity attack. Discussions with insurance brokers has led us to understand that a few different coverages (*e.g.*, a cyber policy, a crime policy, errors and omissions, and fiduciary insurance) may all need to be bundled to provide a comprehensive solution. It is also important to address cyber breaches that can occur at different plan interfaces, for instance, at the trustee, participant, or administrator's interface.

It is never too late to examine your cybersecurity procedures and protocols. We also cannot stress enough that even the best procedures

and plans should be reviewed and revised as necessary given how quickly new technologies emerge and cybercriminals continue to evolve.

Finally, despite the best cybersecurity defenses, there are zero-day attacks that can defeat the best laid plans. Therefore, a fiduciary may look into purchasing an insurance policy or bond to protect against potential loss to the plan and plan participants. Although such coverage is available, the plan fiduciary needs to know exactly what type of coverage it should purchase. Further, a negative factor with respect to insurance coverage is that where the actual cyber-breach occurs may dictate whether the insurer will pay the claim. Unless the cyber-breach occurs at the plan sponsor's interface, the claim may be refuted. Thus, even if a plan sponsor has adequate insurance coverage, the insurer may refuse to pay a claim if the breach happens at the site of the service provider, or if the plan participant's negligence led to the breach. It is critical to get counseling on the appropriate cyber insurance plan to cover your specific needs.

NOTES

1. The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time.

2. *https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2011-privacy-and-security-issues-affecting-employee-benefit-plans.pdf*, last accessed March 1, 2018.

3. *https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf*, last accessed March 1, 2018.