Your Next Cybersecurity Breach Will Be Your 401(k) . . . Soon

*David McFarlane and Alice Hall-Partyka, Crowell & Moring LLP**

Imagine you arrive home from work and your house is gone—literally vanished. No fire. No earthquake. One of your major assets gone. Poof. You had locked the doors. The Neighborhood Watch seemed vigilant. How could this happen? Who is responsible?

Now, imagine the same thing happens to your 401(k) account, IRA or pension. One of your major assets gone. Poof. You had locked your account. Your employer seemed vigilant. How could this happen? Who is responsible? The answer in THIS situation, however, is clear. Your plan's fiduciaries are responsible—and personally.

With large-scale cyberattacks on the rise and cybercrime expected to cost $6 trillion annually by 2021,[1] employers need to consider how employee data and corporate assets can be better protected from increasingly varied and adept cyber threats. Retirement plans are certainly no exception—and in fact are arguably more vulnerable. With over $28 trillion[2] (yes trillion) in U.S. retirement assets—all linked to sensitive personal information—retirement plans are a prime target for cyber threat actors. Increasingly they are seeing that pot of gold. In April 2018, the banking and retirement industries' cybersecurity groups formed a joint panel to better develop ways to defend against cyberattacks.[3]

Ironically these cyber breaches risk not only the personal information of plan participants and plan's assets, but also the personal assets of board members, those in the C-Suite and other "fiduciaries" of the retirement plan. And if you think these individual fiduciaries can be indemnified, think again. ERISA[4] prohibits it.

What about D&O coverage? Please. Check your policy. I'm sure you'll be in for a surprise . . . .

CYBERSECURITY LANDSCAPE

Cybercrime is becoming increasingly sophisticated. Cyberattacks are caused by threat actors with differing agendas, whether these are foreign governments, "hacktivists," insiders, or opportunistic criminals. And the attack methods they use also vary—the continuously growing list of ways a company or retirement plan can be hacked is hard to keep up with.

As with other sites, ac-

**Based in Los Angeles, DAVID MCFARLANE is a partner in the Crowell & Moring's Corporate, Health Care, Tax, and Labor & Employment groups. He has more than 20 years of experience in the U.S. and Canada advising on pensions, employee benefits, executive compensation, national and international corporate transactions, bankruptcy reorganizations, securities laws, corporate governance, deferred compensation, and structured finance matters related to the Employee Retirement Income Security Act (ERISA), the Internal Revenue Code, and the Affordable Care Act (ACA).*

ALICE HALL-PARTYKA is an associate in the firm's Corporate and Health Caregroups. Her practice focuses on assisting health care payors and providers on regulatory, compliance, and transactional matters. Alice also advises clients on employee benefit matters related to the Employee Retirement Income Security Act (ERISA) and the Internal Revenue Code.

counts, and files containing large amounts of sensitive information, retirement plans need to ensure under ERISA that they 1) have robust protections in place to secure against cybersecurity breaches and 2) keep their plan documents, third-party contracts, and related systems up to date in order to defend against an ever evolving cyber threat landscape. Plan sponsors also need to consistently monitor these systems and protections—a key fiduciary concept under ERISA.

Retirement plans are especially susceptible to cyber threats because of their use of third party vendors, such as plan administrators, advisors, custodians, transfer agents, and trustees (collectively, "TPAs") that have access to plan assets and underlying confidential information. TPAs are often overlooked in cybersecurity planning. Plan sponsors must ensure that TPAs have comprehensive protections and response plans in place. Often we find that retirement plan and TPA contractual policies, procedures and indemnifications are outdated or non-existent when it comes to cybersecurity. Many significant cybersecurity breaches have occurred under the watch of TPAs and not the plan sponsors or employers. In a recent survey by the Ponemon Institute,[5] fifty-six percent of surveyed companies experienced a data breach caused by a third party, but only seventeen percent felt that third party risk was effectively managed.

Plan sponsors must ensure they have appropriate procedures and protections in place to secure plan assets and information from cyberattacks, both within their own system and in the systems of the third parties with which they contract. Similarly, breaches can occur when plan participants are "phished" for passwords and other personal information. But ERISA fiduciaries shouldn't think they are off the hook from any fiduciary liability in these situations. Proper multi-step security protections and plan participant education are also part of a plan fiduciary's responsibility.

LITIGATION AND ENFORCEMENT

Unfortunately, a data breach is only the first hit for hacked employers. Following revelation of a cyber breach, employers and their officers and directors are often sued by a range of parties—attorney general offices, the Federal Trade Commission, consumers, shareholders, employees, and financial institutions. And the related financial penalties can be high.

In March 2018, Yahoo Inc. proposed an $80 million settlement to resolve a class action suit brought by Yahoo Inc. investors against the company and its officials in relation to 2013 and 2014 breaches of users' personal information.[6] A month later, the SEC imposed a $35 million fine on the company as a penalty for how it handled the attack, the first instance of a public company being penalized for its handling of a cybersecurity breach.[7] The company is still facing a lawsuit from data breach victims. The plaintiffs argue such breach affected all 3 billion users of the company.[8]

The various avenues for litigation and enforcement in response to the Yahoo breach emphasize the risks and penalties for a company that has suffered a cyber breach. BUT, where the attack is on a retirement plan, there is an additional litigation basis for an aggrieved class of plan participants and beneficiaries—breach of ERISA's strict fiduciary duties.

ERISA FIDUCIARY DUTIES

Under ERISA, directors, officers, and other employees who exercise discretionary authority or control over plan management, administration, or disposition of plan assets

are considered fiduciaries and as such owe particular fiduciary duties to the plan's participants and beneficiaries.[9] Whether a director, officer, or employee is considered a fiduciary is a fact-based test—in other words it depends on the plan management, control, or duties he or she performs. It has nothing to do with an individual's title vis-à-vis the retirement plan.

What are the fiduciary's duties? To start, each fiduciary has the duty to act solely in the interests of plan participants and the duty to act with "care, skill, prudence, and diligence."[10] In the cybersecurity context, fiduciaries may not be acting with that "prudence" and "diligence" if they are not considering, implementing, and monitoring robust procedures and protections to secure plan assets and data. Even if a fiduciary is not involved in cybersecurity management, he or she could still be liable under ERISA as a "co-fiduciary" for knowingly participating in a breach, concealing a breach, or even simply not acting to correct a breach.[11]

What's at risk for these employees, officers, and directors? A lot. Under ERISA, a fiduciary is personally liable for any breaches of fiduciary duties.[12] Yup, his or her personal assets are at risk for what may happen under the company's 401(k) or other retirement, health, or welfare plan. And it gets worse. Plan sponsors/employers and retirement plans are prohibited from indemnifying them against the risk.[13]

So what about directors and officers (D&O) liability insurance? It's permitted under ERISA but often—if it even exists—It's insufficient in amount or there's an ERISA "carve-out" from the policy. Companies typically maintain D&O insurance to cover directors and officers for claims made against them while serving on a board of directors or as an officer. However, D&O insurance can be outdated and may insufficiently cover potential risk for fiduciary duty breaches relating to cyber breaches and in particular anything related to employee benefit plans that are subject to ERISA. While carriers are increasingly offering stand-alone cyber insurance policies, these policies usually do not provide any protection against ERISA fiduciary duty breaches.

APPROPRIATE CYBERSECURITY PROCEDURES AND PROTECTIONS

Retirement (and health) plan sponsors should immediately ensure that their employee benefit plans have appropriate written procedures, protections, action plans, and other safeguards to secure plan assets and plan participant data. To do otherwise may risk the personal assets and property of the members of the board of directors, the CEO, CFO, Chief Human Resources Officer, committee members, and certain employees who have some discretion, control, or management authority over the employee benefit plan.

Whether or not their duty of prudence under ERISA has been breached will largely depend on whether the fiduciary can show that he or she engaged in procedural due diligence before taking the questioned action. In other words, it is not just the decision that matters—it is the process. Employees, officers, and directors should be able to show that they adequately considered and assessed cybersecurity procedures and ensured that other providers were meeting these requirements.

Fiduciaries also need to ensure that TPAs who receive data and assets from the employer or employee benefit plan are appropriately protecting these assets (and plan data is considered an "asset"). The duty of prudence requires that plan fiduciaries: 1) select plan service providers carefully, 2) ensure they have ap-

propriate cybersecurity plans in place, 3) check that contracts contain current and appropriate language, and 3) regularly oversee and monitor such providers.

Since breaches also arise from "phishing" of plan participants for passwords and other personal information, proper multi-step security protections and plan participant education are an additional part of a plan fiduciary's responsibility. Even where plan participants took inadequate precautions with their own information, fiduciaries will likely be blamed after the breach for providing inadequate training or having an inadequate cybersecurity system.

Unfortunately there are few statutory guidelines on the appropriate cybersecurity procedures for employee benefit plans. The Department of Labor prescribed certain measures that employee benefit plan administrators must take when electronically distributing documents, but not much more. Under federal regulations, the plan administrator must "take[] appropriate and necessary measures reasonably calculated" to ensure that documents are sent in a way that ensures receipt by the appropriate sender and protects the confidentiality of personal information.[14] Even though the statutory guidance is limited, the increase in cybersecurity risks and attacks has led various stakeholders to consider what companies should be doing to protect their data.

CYBERSECURITY BEST PRACTICES

Government and industry stakeholders have developed various best practices and guidelines that, while not binding on retirement and healthcare plans, are useful.

In 2002, the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY Act) was enacted to encourage the use of anti-terrorism products and technologies in civilian settings.[15] The SAFETY Act limits liability for companies using technologies certified by the Department of Homeland Security. Incorporating these certified technologies could provide plans additional protection against cyber threats.

In response to the Obama Administration Executive Order on "Improving Critical Infrastructure Cybersecurity,"[16] government and private sector stakeholders collaborated to release in 2014 voluntary cybersecurity management standards for companies owning or operating critical infrastructure.[17] Organizations were encouraged to adapt the three-part framework to their own business drivers, threats, resources, and risk tolerance.

In a 2016 report to the Secretary of Labor, the Advisory Council on Employee Welfare and Pension Benefit Plans emphasized the particular risks for retirement plans and encouraged plans to develop customized cybersecurity frameworks and strategies.[18] Notably, the report advised plans contracting with service providers to use service providers with vetted policies and SAFETY Act designations and to include in the contracts clearly defined security and data access obligations, consistent monitoring and audit obligations, and regulatory compliance stipulations.

In 2017, the American Institute for CPAs (AICPA) released a cybersecurity risk management reporting framework to enable organizations to proactively consider cybersecurity risk management and to communicate these activities with stakeholders.[19]

CREATING YOUR OWN CYBERSECURITY RISK MANAGEMENT PROCEDURES

401(k) and other pension and health plan fiduciaries should take the following actions, and soon:

- Undertake a legal review

and modify benefit plan documents where necessary in order to ensure there are cybersecurity provisions and mechanisms to best protect the interests, privacy, and assets of plan participants and beneficiaries;

- Review third-party providers contacts and negotiate revisions where necessary to best protect the plan and plan sponsor in situations of cyber breaches arising from TPAs, including timely notification and robust indemnification provisions;
- Review D&O insurance contracts to ensure proper ERISA coverage with no restrictive "conditions";
- Develop a cybersecurity plan that contains procedures for timely notification to plan participants and regulatory authorities where required;
- Ensure board of directors and pension committee minutes reflect action taken including monitoring;
- Train plan fiduciaries annually on their ERISA duties, including those relating to cybersecurity; and
- Implement advanced safeguards and training for plan participants.

ERISA plan fiduciaries, don't wait until your house is gone—literally.

NOTES:

[1]Steve Morgan, Cybercrime Damages Expected to Cost the World $6 Trillion by 2021, CSO Online (Aug. 22, 2016), *available at*: https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

[2]Frequently Asked Questions About 401(k) Plan Research, Investment Company Institute (March 2018), *available at*: https://www.ici.org/policy/retirement/plan/401k/faqs_401k.

[3]Allison Bell, Retirement Services Group Forms Data Security Alliance, ThinkAdvisor (April 25, 2018), *available at*: https://www.thinkadvisor.com/2018/04/25/retirement-services-group-forms-data-security-alli/?slreturn=20180403155259.

[4]Employee Retirement Income Security Act of 1974 ("ERISA").

[5]Opus & Ponemon Institute Announce Results of 2017 Third Party Data Risk Study: 56% of Companies Experienced data Breach, Yet Only 17% Are Prepared to Mitigate Risk (Sept. 27, 2017), *available at*: https://www.opus.com/about/press_releases/opus-ponemon-announce-results-of-2017-third-party-data-risk-study/.

[6]Judy Greenwald, Settlement Proposed in Yahoo Data Breach Securities Litigation, Business Insurance (March 6, 2018), *available at*: http://www.businessinsurance.com/article/20180306/NEWS06/912319665/Settlement-proposed-in-Yahoo-data-breach-securities-litigation.

[7]Dave Michaels, Yahoo's Successor to Pay $35 Million in Settlement Over Cyberbreach, Wall Street Journal (April 24, 2018), *available at*: https://www.wsj.com/articles/yahoos-successor-to-pay-35-million-in-settlement-over-cyber-breach-1524588040.

[8]Jonathan Stempel, Data Breach Victims Can Sue Yahoo in the United States: Judge, Reuters (March 12, 2018), *available at*: https://www.reuters.com/article/us-verizon-yahoo-breach/data-breach-victims-can-sue-yahoo-in-the-united-states-judge-idUSKCN1GO1TL.

[9]29 U.S.C. § 1002(21)(A).

[10]29 U.S.C. §§ 1104(a) & 1106.

[11]29 U.S.C. § 1105.

[12]29 U.S.C.A. § 1109.

[13]29 U.S.C.A. § 1110.

[14]29 C.F.R. § 2520.104b-1(c).

[15]6 U.S.C.A. §§ 441 et seq.

[16]Exec. Order No. 13,636: Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013), *available at*: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[17]Nat'l Inst. of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at*: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[18]Advisory Council on Employee Welfare and Pension Benefit Plans, Report to the Honorable Thomas E. Perez, United States Secretary of Labor, Cybersecurity Considerations for Benefit Plans (Nov. 2016), *available at*: https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

[19]AICPA, AICPA Unveils Cybersecurity Risk Management Reporting Framework (April 26, 2017), *available at*: https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurity-risk-management-reporting-framework.html.