# New Cybersecurity Insights From ERISA Rulings, DOL Advice

By **Richard Nowak and Alexander Vitruk** (June 14, 2021)

Richard Nowak

Alexander Vitruk

Cybersecurity has become critically important to plan sponsors, plan administrators and plan participants. With retirement plans holding an estimated $9.3 trillion in assets as well as sensitive information for approximately 140 million plan participants,[1] retirement accounts are especially attractive targets for cyber-enabled fraud.

For instance, sophisticated phishing email schemes have proliferated during the COVID-19 pandemic, threatening retirement accounts.[2] Ever-expanding technology connecting data and people has also opened the door to bad actors.[3]

This article explores the expanding intersection of the Employee Retirement Income Security Act[4] and cybersecurity issues, focusing on recent court decisions as well as guidance from the U.S. Department of Labor.

**ERISA Claims Based on Cybersecurity Issues**

As more and more cyber breaches pervade the industry, plan sponsors and administrators should be cognizant of fiduciary risk.

As litigation has already shown, a new argument in ERISA cases is that ERISA's duty of prudence — which obligates fiduciaries to act with the care, skill, prudence and diligence of a prudent man when satisfying their obligations to the plan — requires fiduciaries to take appropriate steps to safeguard sensitive participant data and participants' benefits.[5] While these are relevantly new issues, courts around the country have started shaping the intersection of ERISA and cybersecurity.

In Leventhal v. MandMarblestone Group LLC,[6] for instance, the U.S. District Court for the Eastern District of Pennsylvania in May 2019 concluded that the plaintiff had pled a plausible fiduciary breach related to cybersecurity incidents.

In Leventhal, a participant in the Leventhal Sutton & Gornstein 401(k) profit-sharing plan allegedly withdrew money from his plan account by emailing a withdrawal request form that was intercepted by unknown criminals who posed electronically as his office administrator and sent fraudulent withdrawal forms to the defendants — the alleged plan fiduciaries.[7] The fraudulent withdrawal forms purportedly requested that the defendants send the participant's account funds to a bank account that did not belong to the plaintiff and had never been used by him.

The district court found that the plaintiffs had plausibly stated an ERISA breach of fiduciary duty claim because they alleged that they had obtained documents from the defendants showing that the defendants were aware of the peculiar nature and frequency of the fraudulent withdrawal forms, but failed to alert the plaintiffs or verify the requests.[8] The district court also credited the plaintiffs' allegations that the defendants had failed to implement the typical procedures and safeguards used to notify participants of strange requests and/or verify the requests.[9]

An April 2021 decision from the U.S. Court of Appeals for the Ninth Circuit, Pruchnicki v. Envision Healthcare Corp.,[10] may also have broader implications for ERISA matters stemming from cybersecurity issues. Although she did not allege any claims under ERISA, the plaintiff alleged four categories of injury stemming from a data breach[11] of the defendants' systems:

- Lost time spent reviewing consumer credit reports, obtaining new credit cards, checking financial accounts, and answering an increased number of spam calls;
- Emotional distress, including stress, nuisance and annoyance from dealing with the effects of the breach; worry, anxiety and hesitation when applying for new credit cards; and concern that damage to her creditworthiness could affect her ability to obtain credit for her business;
- Imminent and certainly impending injury flowing from potential fraud and identity theft; and
- Diminution in value of her personal and financial information.[12]

The Ninth Circuit affirmed the district court's dismissal of the case on the ground that, although the plaintiff alleged sufficient injury in fact to support standing,[13] she had failed to establish compensable damages, or out-of-pocket expenses. The Ninth Circuit explained that the plaintiff cited no authority recognizing lost time as a cognizable injury, failed to assert the existence of any physical injury or illness, and failed to allege that her personal information actually lost value.

This decision may be instructive for ERISA matters, at least within the Ninth Circuit, given that, to state an ERISA fiduciary breach claim, a plaintiff must establish harm.[14] The types of harm identified in Pruchnicki — e.g., lost time, emotional distress, diminution of value of personal information — may not be sufficient to sustain a fiduciary breach claim.

There are also a growing number of cases at the intersection of ERISA and cybersecurity. For example, participants have asserted ERISA claims in circumstances involving alleged identity theft and unauthorized distributions from their retirement accounts.[15]

Plan service providers and fiduciaries to retirement plans should be cognizant of not only ERISA's fiduciary requirements and the growing body of litigation involving participants who have suffered retirement plan losses due to cyberattacks, but also applicable state laws that provide for disclosure of personal or private information, such as North Carolina and California. Indeed, state attorneys general have been active in enforcing these laws in cyber breach matters.[16]

Given the DOL's current focus on cybersecurity issues, discussed below, and the likelihood that cybersecurity attacks on retirement accounts will persist and become more sophisticated, we expect to see an increase in the number of ERISA cases in this area.

**Recent Guidance From the DOL**

On April 14, the DOL **published written guidance** on cybersecurity issues concerning plan sponsors, plan fiduciaries, record-keepers and plan participants. Acknowledging that ERISA requires plan fiduciaries to take appropriate precautions to mitigate the risks of internal and

external cybersecurity threats to participants and assets, the DOL issued its guidance in three parts:

- Tips for hiring a service provider with strong cybersecurity practices;
- Cybersecurity program best practices; and
- Online security tips.[17]

### *Hiring a Service Provider With Strong Cybersecurity Practices*

The DOL guidance offers various suggestions for hiring and monitoring a service provider to help plan fiduciaries meet their responsibilities under ERISA. Those tips included:

- Compare the service provider's information security standards, practices and policies, audit results to standards adopted by other financial institutions, and seek providers that engage a third-party auditor to review and validate its program.

- Seek contract provisions that give the right to review audit results.

- Evaluate the provider's track record in the industry with respect to security incidents, litigation and legal proceedings.

- Inquire about past security breaches and how the provider responded.

- Find out if the provider's insurance policies would cover losses covered by cybersecurity and identity theft breaches.

- Ensure that the contract requires ongoing compliance with cybersecurity and information security standards; avoid contract provisions that limit the service provider's responsibility; and include contract provisions that would enhance cybersecurity protection for the plan and its participants.[18]

Although the DOL's cybersecurity suggestions are memorialized in subregulatory guidance, as opposed to a formal regulation, plan sponsors and fiduciaries should keep this guidance in mind when hiring and retaining plan service providers.

Accordingly, plan sponsors and fiduciaries should consider reviewing their current hiring practices and service provider contracts to see whether they meet the suggested standards. Among other things, plan sponsors and fiduciaries should carefully review any contractual language limiting the service provider's liability and obligations in the event of a breach.

And, consistent with their existing monitoring efforts, plan sponsors and fiduciaries should consider engaging in periodic third-party audits and reviews of the service provider's track record — e.g., security incidents, litigation, etc. Indeed, cybersecurity practices should be a focus of any request for proposal and part of any ongoing reviews of service providers — e.g., requests for proposals should seek information about data security and data transmittal policies, insurance coverage, etc.

Future plaintiffs may rely on the DOL's recent guidance in arguing that there is a duty to safeguard plan assets against unauthorized withdrawals and that plan fiduciaries also have a duty to take sufficient steps to properly select and monitor a service provider's

cybersecurity policies.

On the flip side, plan fiduciaries who undertake those steps may have a stronger defense against such actions. Moreover, those steps should be accurately and thoroughly reflected in fiduciary committee minutes and materials to document a prudent process and thereby minimize risk of fiduciary liability.

***Cybersecurity Program Best Practices***

With respect to cybersecurity program best practices, the DOL provides recommendations to service providers to assist them in developing and maintaining an effective cybersecurity program.

Though these best practices are directed toward service providers, the DOL also emphasizes that: "Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks," which includes making "prudent decisions on the service providers they should hire."

The DOL's recommendations include, among other things:

- Have a formal, well-documented cybersecurity program that is reviewed annually, approved by senior leadership, explained effectively to users, and reviewed by an independent auditor.
- Conduct and document prudent annual risk assessments.
- Have strong access control procedures, including with respect to authentication and authorization.
- Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.
- Conduct periodic cybersecurity awareness training, at least annually for all personnel and update it to reflect risks identified by the most recent risk assessment.
- Implement strong technical controls in accordance with best security practices, including routine data backup and patch management, up-to-date hardware, software, firmware and antivirus software, and network segregation.[19]

Plan service providers should consider incorporating language into their service contracts on compliance with these recommended best practices going forward. Moreover, as discussed above, the recent ERISA matters based on cyberattacks have generally involved cyber criminals posing as participants, often calling into the record-keeper's service center to obtain participant data.

As such, having an effective customer call center authentication process is important.[20] Customer service representatives should be trained to ask callers to verify items such as their date of birth, home address and other personal identifying information. A more sophisticated customer call center authentication process may involve tokens associated with a caller's phone or carrier, or a multifactor authentication system that can understand the characteristics of certain sounds that can be translated into a voice print.[21]

Plan fiduciaries should monitor whether service providers have such practices in place. This is especially important in the wake of any breach. Indeed, cybersecurity breaches often involve service providers who handle day-to-day administration for retirement plans.

For example, NOW: Pensions, a UK pensions provider, was the victim of a data breach by an unknown third party during a three-day period in December 2020. It resulted in the personal information of 30,000 customers being posted on the internet, and the company blamed the data breach on one of its service providers.[22]

When faced with such a breach, an organization may be inclined to terminate its service provider. In some cases, there may be grounds to terminate the relationship — e.g., the provider may have failed to comply with the parties' contract or applicable law. But there may also be compelling reasons to retain the provider — e.g., there is a dependable relationship and the provider's unique products or services are critical to the organization.

Plan sponsors and administrators should consider different factors in making such a consequential decision to determine whether it is in the best interest of the plan and its participants. They should also carefully evaluate and document — and revise as appropriate — their measures and processes in the wake of any breach.

***Online Security Tips***

Finally, the DOL offered online security tips to plan participants to help reduce their own risk of retirement account fraud and loss. Those tips include:

- Register, set up and routinely monitor online accounts.
- Use strong and unique passwords.
- Use multifactor authentication;
- Keep personal contact information current.
- Close or delete unused accounts.
- Be wary of free Wi-Fi.
- Beware of phishing attacks.
- Use anti-virus software and keep apps and software current.
- Know how to report identity theft and cybersecurity incidents.[23]

Although the DOL's online security tips are primarily directed toward participants, plan sponsors and fiduciaries should consider providing and documenting education on cybersecurity issues to their participants.

For instance, they could provide clear guidance in the summary plan description, regularly issue best practices notices to participants, and organize educational seminars.

Not only is cybersecurity education important to help participants protect their own financial well-being, taking active steps to help participants understand potential cybersecurity and data privacy risks may reduce the risk of litigation against the plan sponsor and the plan's fiduciaries and help them defend against future claims.

**Conclusion**

Cybersecurity has become an area of critical importance to plan sponsors, plan administrators and plan participants.

Plan sponsors and administrators are well advised to follow the growing body of litigation involving participants who have suffered retirement plan losses due to cyberattacks, and to evaluate their cybersecurity programs, protocols and contracts against the DOL's recent three-part guidance.

---

*Richard E. Nowak is a partner and Alexander Vitruk is an associate at Mayer Brown LLP.*



[1] U.S. Dep't of Labor, News Release, US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, Plan Participants (April 14, 2021), available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.

[2] See Alessandra Malito, Hackers Are Ramping Up Attacks on Retirement Accounts – How to Keep Yourself Safe, MarketWatch, (Feb. 6, 2020), available at https://www.marketwatch.com/story/how-to-keep-your-retirement-accounts-safe-2020-01-28.

[3] See Rebecca Moore, Expansion of Technology Will Increase Cyber Security Threats, Plan Sponsor, (Feb. 15, 2019), available at https://www.plansponsor.com/expansion-technology-will-increase-cyber-security-threats/.

[4] 29 U.S.C. § 1001 et seq.

[5] See ERISA § 404(a)(1)(B), 29 U.S.C. § 1104(a)(1)(B).

[6] Leventhal v. MandMarblestone Grp. LLC , No. 18-CV-2727, 2019 WL 1953247 (E.D. Pa. May 2, 2019).

[7] 2019 WL 1953247 at *2. The named plaintiffs were participant Jess Leventhal, Leventhal Sutton & Gornstein 401(k) Profit Sharing Plan, and Leventhal Sutton & Gornstein, Attorneys at Law.

[8] Id. at *6.

[9] Id.

[10] Pruchnicki v. Envision Healthcare Corp ., 845 F. App'x 613 (9th Cir. April 21, 2021).

[11] Plaintiff had provided her personal and/or financial information to defendants, according to the underlying complaint. See Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1229 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021).

[12] Pruchnicki, 845 F. App'x 613.

[13] The district court held, and the defendants conceded, that the plaintiff had standing based on allegations of future harm. Pruchnicki v. Envision Healthcare Corp., 439 F. Supp.

3d 1226, 1231 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021).

[14] See, e.g., Allen v. GreatBanc Tr. Co ., 835 F.3d 670, 678 (7th Cir. 2016); see also Wise v. MAXIMUS Fed. Servs., Inc ., 445 F. Supp. 3d 170, 196 (N.D. Cal. 2020) (same).

[15] See, e.g., Bartnett v. Alight Solutions, LLC, et al. , No. 20-CV-02127, 2021 WL 428820 (N.D. Ill. Feb. 8, 2021); Berman v. Alight Solutions, LLC, et al., No. 4:19-cv-06489-JST (N.D. Cal., filed Oct. 9, 2019).

[16] See, e.g., Press Release, Arizona Attorney General, Attorney General Mark Brnovich Files Lawsuit Against Google Over Deceptive and Unfair Location Tracking, (May 27, 2020), available at https://www.azag.gov/press-release/attorney-general-mark-brnovich-files-lawsuit-against-google-over-deceptive-and-unfair.

[17] U.S. Dep't of Labor, News Release, US Department of Labor Announces New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, Plan Participants (April 14, 2021), available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.

[18] U.S. Dep't of Labor, Tips for Hiring a Service Provider with Strong Cybersecurity Practices (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf.

[19] U.S. Dep't of Labor, Cybersecurity Program Best Practices (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

[20] Forrester Research, Best Practices: Customer Call Center Authentication, (March 22, 2019), available at https://www.forrester.com/report/Best+Practices+Customer+Call+Center+Authentication/-/E-RES141457.

[21] See Ben Rizzuto, Janus Henderson Investors, Protecting Plan Participants from Cyberthreats in the Age of Remote Working, (Oct. 28, 2020), available at https://www.janushenderson.com/en-us/advisor/article/protecting-plan-participants-from-cyberthreats-in-the-age-of-remote-working/.

[22] See Miles Brignall, Data Breach Hits 30,000 Singed Up to Workplace Pensions Provider, The Guardian, (Dec. 23, 2020), available at https://www.theguardian.com/technology/2020/dec/23/data-breach-hits-30000-signed-up-to-workplace-pensions-provider.

[23] U.S. Dep't of Labor, Online Security Tips (April 14, 2021), available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf.