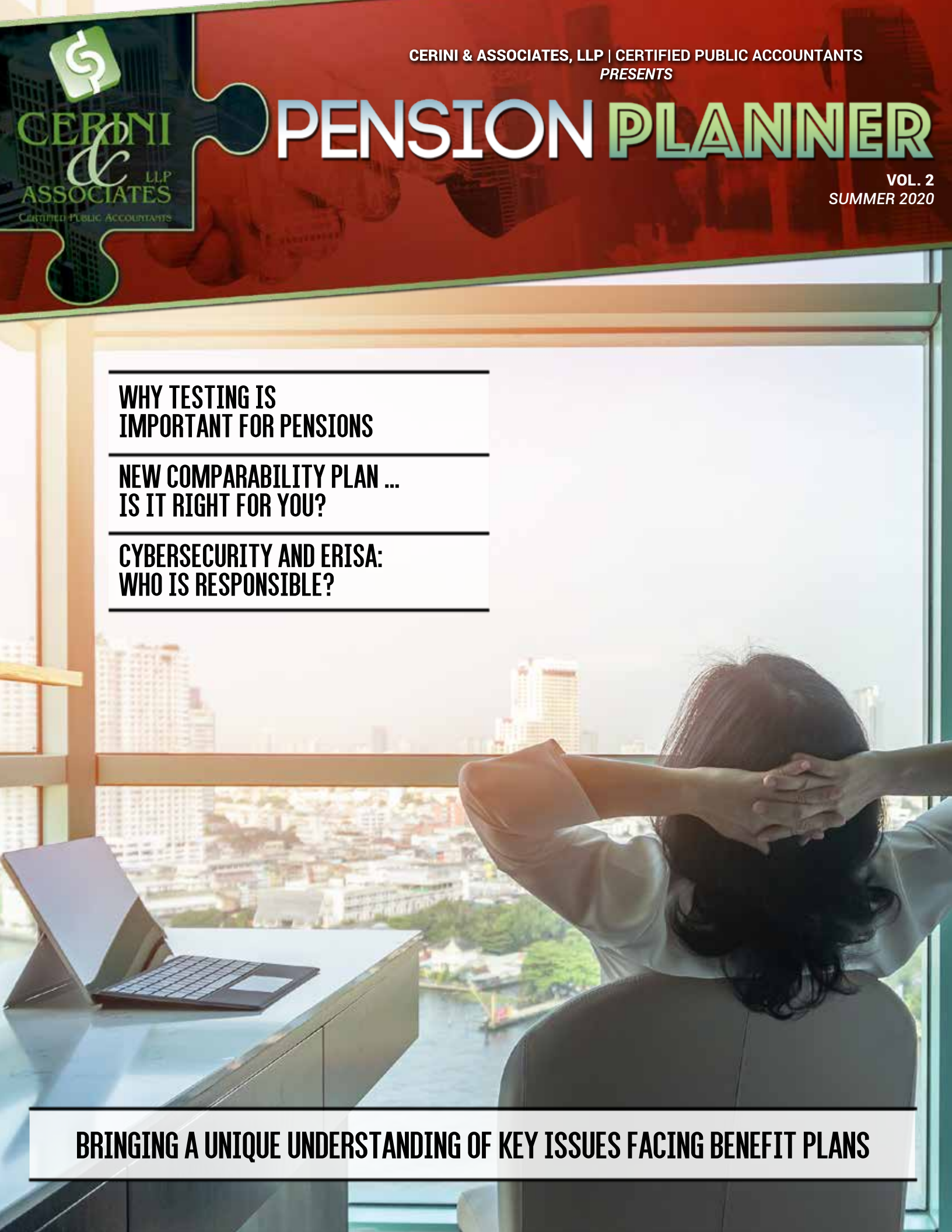
CERINI & ASSOCIATES, LLP | CERTIFIED PUBLIC ACCOUNTANTS

PRESENTS

PENSION PLANNER

VOL. 2

SUMMER 2020



WHY TESTING IS IMPORTANT FOR PENSIONS

NEW COMPARABILITY PLAN ... IS IT RIGHT FOR YOU?

CYBERSECURITY AND ERISA: WHO IS RESPONSIBLE?

BRINGING A UNIQUE UNDERSTANDING OF KEY ISSUES FACING BENEFIT PLANS

FROM THE EDITOR - TANIA QUIGLEY, CPA

We hope everyone is staying safe and sane, which has not been easy during the COVID-19 pandemic.

There has been so much information coming out during the last few months with respect to employee benefits, getting back to work, fiscal issues, and more, that it's been challenging to stay on top of everything, and I'm sure your company's pension plan isn't a top priority right now. Even so, it is essential to focus on your pension periodically to ensure that you are in compliance and that your employee's financial future is being considered. In that vein, welcome to the 2020 edition of the Pension Planner, our annual newsletter focused on helping you manage your pension plan more effectively.

If you have not already had the conversation with your TPA, there are two new provisions that you will need to know about: the SECURE Act and the CARES Act.

The SECURE Act has the following key provisions:

- *Provides for pooled employer plans (an open form of multi-employer plan)*
- *Makes plan notice provisions and plan amendments easier and requires less lead time*
- *Makes the plan easier for employees to participate (either 1,000 hours of service in a year or three years of 500 hours of service)*
- *Added new eligible withdrawals of up to $5,000 for childbirth and adoption expenses*
- *The starting age for minimum distributions has been increased from 70.5 to 72*
- *Related plans can file a consolidated form 5500*
- *Penalties for lack of compliance with IRS and ERISA requirements have significantly increased*

Unlike the SECURE Act, which includes some mandatory provisions that a plan must adopt, The CARES Act is elective and contains the following provisions:

- *Enhanced loans (the lesser of $100,000 or 100% of a qualified participants account balance)*
- *Permitted distributions up to $100,000 during 2020 to a qualified individual (not subject to 10% penalty and taxed over 3 years)*
- *Potential for hardship withdrawals for COVID related hardships (medical expenses, eviction prevention, foreclosure, etc.)*

Under the CARES Act, a qualified participant is one who:

- *Was diagnosed with COVID or their spouse or dependent was diagnosed*
- *Experienced adverse financial consequences as a result of the pandemic (quarantined, laid off, furloughed, reduced work hours, unable to work due to childcare issues)*
- *Forced to close or reduce hours of a business owned or operated by the individual due to COVID*

These are just quick summaries of these Acts, and I would be more than happy to have a deeper conversation if you have specific questions.

Please take the time to flip through this newsletter, as there are some really important articles focused on the importance of plan testing, cybersecurity and your exposure within your pension, and the new comparability plan, a plan with a lot of flexibility that may be a perfect fit for your company.

We know that managing a pension plan can be intimidating and you don't always know what you don't know. That's why surrounding yourself with professionals (*accountants, lawyers, trustees, and TPAs*) who are knowledgeable is so important. Please consider us a resource. Stay connected!

CONTRIBUTORS

EDITOR

TANIA QUIGLEY, CPA
CERINI & ASSOCIATES, LLP
DIRECTOR, AUDIT

WRITERS

MATTHEW HECKER, MS
CERINI & ASSOCIATES, LLP
SENIOR ACCOUNTANT

KEN CERINI, CPA, CFP, FABFA
CERINI & ASSOCIATES, LLP
MANAGING PARTNER

JENNY L. HOLMES
ASSOCIATE
NIXON PEABODY LLP

ASSOCIATE EDITOR

KEN CERINI, CPA, CFP, FABFA
CERINI & ASSOCIATES, LLP
MANAGING PARTNER

PAGE LAYOUT & DESIGN

KRISTINA LAINO
CERINI & ASSOCIATES, LLP
GRAPHIC DESIGNER

CERINI & ASSOCIATES LLP
CERTIFIED PUBLIC ACCOUNTANTS

3340 VETERANS MEMORIAL HWY., BOHEMIA, NY 11716 | (631) 582-1600 | WWW.CERINICPA.COM

WHY TESTING IS IMPORTANT FOR PENSIONS

As auditors, we are always busy performing different types of testing, especially controls and compliance-based test work. While there is a common stigma about auditors and audits in general, and they have a *"gotcha"* sort of mentality, there is a tremendous benefit that a company can derive from the work they perform. The truth is, our goal is to ensure that companies and organizations are complying with rules and regulations so that they can avoid costly errors, especially when it comes to defined contribution pension plans.

One test that we perform is called the participant test. This is an overall test of plan participants to ensure that eligibility requirements are met per the plan document, contributions are properly calculated and allocated to employees based upon their eligibility and withholding requests, and demographic information transmitted to the plan's custodian is complete and accurate. While most of these processes are handled electronically, we want to ensure that they are still handled properly and that investment selections and allocations are correct.

Another compliance-based test we perform considers the timely remittance of contributions by the Plan Sponsor to the custodian of the funds. This is important because the **Department of Labor (DOL)** requires the employer to deposit deferrals to the custodian as soon as the employer can. Deposits can never be later than the 15th business day of the following month, which is a rule set as the maximum deadline. This however, is not a safe harbor. Having the contributions remitted timely ensures that the employer is following DOL regulations while reducing the potential for lost earnings to participants due to a time lag incurred by the employer. If contributions aren't timely remitted, the employer has to contribute to the Plan the amount that each employee had in lost earnings due to the late remittance.

We also review general compliance test results performed for standard defined contribution plans. These include nondiscrimination tests in elective deferrals, employer contributions, availability of benefits, top-heavy tests, and limits on the maximum elective deferrals allowed by the **Internal Revenue Service (IRS)** each year. Top-heavy tests ensure that participants who are key employees do not receive a disproportionate amount of benefits compared to non-key employee participants. All of these compliance-based tests provide assurance that the plan is following IRS regulations so that it can remain as a qualified plan for participants.

We perform all of these tests, and more, annually to make sure that employers are in line with guidance and compliance matters as set by authoritative bodies such as the DOL and IRS. After all, if the plan is out of compliance, you would rather hear from us, your auditors, when you can self-correct, as opposed to from a governmental agency.

MATTHEW HECKER, MS
SENIOR ACCOUNTANT

NEW COMPARABILITY PLAN...

IS IT RIGHT FOR YOU?

Pension plans should be an important part of every business' benefits package. Not only do they let business owners/executives and employees to set aside funds for their retirement, but they provide the added ability for companies to assist in the process and make contributions on behalf of their staff, to help them better position themselves for retirement. There are many different retirement plans available for companies to set-up, but one of the ones that offer businesses some of the most flexibility is the **New Comparability Plan ("NCP")**.

NCP BACKGROUND:

A NCP is a profit-sharing plan strategically used by many companies to be able to direct pension contributions to specific individuals, programs, departments, class of workers, etc., within certain limitations. What this means is, if the plan doesn't run into a non-discrimination issue, an employer can contribute a different percentage of each employee's salary, providing a tremendous level of flexibility to the plan sponsor. This would allow companies to potentially direct pension contributions to more profitable departments, sales teams, deficit funded programs, etc.

NONDISCRIMINATION REQUIREMENTS:

NCP's are *"cross-tested"* plans that are subject to nondiscrimination rules which requires the contribution on behalf of each plan participant to be actuarily projected, with interest, to retirement age and converted to an annual pension benefit expressed as a percentage of current compensation (*the "equivalent benefit accrual rate"*). Since the nondiscrimination testing considers resources at retirement age, an NCP plan tends to be more favorable to older individuals (*such as company or organizational leadership*), making it easier to meet nondiscrimination testing, even with little or no contributions going to certain employees.

In order for an NCP to use cross-testing, the IRS requires it to meet one of 3 requirements: **(i)** Broadly available allocation rates, **(ii)** provide a *"gradual age or service schedule"* or a *"uniform target benefit allocation,"* or **(iii)** satisfy a gateway condition. These requirements are very complex and should be discussed with your third-party administrator or plan consultant to ensure that you can meet these requirements.

APPLICABLE LIMITATIONS:

As with all profit-sharing plans, the maximum employer contribution is limited to 25% of the eligible compensation paid to participants in the NCP. Eligible compensation levels change on an annual basis, so once again, you should discuss this with your accountant or third-party administrator.

CONCLUSION:

A NCP may be an attractive option for a company's pension plan, depending on its employee demographics, spending patterns, and compensation structure. Some of the negative aspects that an employer must consider are:

- *Start-up fees associated with the determination and establishment of an NCP*
- *Additional annual fees for cross-testing and top-heavy testing requirements*
- *Overall increased annual administrative fees*

Even so, if properly designed, an NCP can provide a significant level of benefits and flexibility to a company, including:

- *Flexibility with respect to pension contributions and the ability to target where those contributions go;*
- *Flexibility to determine contribution amounts on a year-to-year basis, depending on profits and business objectives*
- *A tax deduction for qualified pension contributions;*
- *Deferral of taxation of contributions, including earnings, until the funds are ultimately distributed*
- *NCP provisions can be added to an existing 401(k) plan*

Plan sponsors should consider whether or not an NCP is the right option for them.

KEN CERINI, CPA, CFP, FABFA
MANAGING PARTNER

CYBERSECURITY AND ERISA:
WHO IS RESPONSIBLE?

Cybersecurity risks are not new. We've been dealing with data breaches for years, and if we've learned one thing, it's that hackers are smart. Hackers can infiltrate even the most complex security systems in the pursuit of personal information. It was only a matter of time until retirement plans, rich with personal information and money, fell victim to data breaches too. And like most companies navigating the aftermath of a data breach, retirement plan sponsors and service providers can easily find themselves in the midst of intense litigation.

Now, with the implementation of the **Coronavirus Aid, Relief, and Economic Security Act ("CARES Act")**, plan sponsors and service providers are seeing an influx of participant requests for distributions and loans. Unfortunately, this presents an opportunity for cybercriminals to take advantage of easier distribution rules and overwhelmed service providers. Combined with the relatively easy access to money, retirement plans are more desirable than ever for cybercriminals.

Recent litigation illustrates the complexity of issues that can arise when a retirement plan is breached. With so many players, including affected participants, plan sponsors, administrators, and recordkeepers, responsibility becomes a game of finger-pointing and *who-did-it?* From these cases, all parties can learn about their duties to protect personal information.

Berman v. Estee Lauder, Inc. et al.

In October 2019, a participant in the **Estee Lauder Companies 401(k) Savings Plan (the "Lauder Plan")** filed a complaint against the plan sponsor, the employee benefits committee, Alight Solutions LLC, as recordkeeper, and the Lauder Plan's custodian, claiming breaches of the fiduciary duties of loyalty and prudence.

According to the complaint, the participant had more than $90,000 in her account balance as of June 30, 2016. In three withdrawals, of which the participant only received two *"confirmation of payment letters"* via postal mail, the participant's account was all but drained. The participant also alleges she made at least 23 phone calls to the recordkeeper's customer service center. Ultimately, the participant was told that the investigation was complete, no money had been recovered, and that the participant's account balance would not be made whole. Notably, the participant claims that no one from the plan sponsor or the employee benefits committee ever contacted her concerning this theft.

The complaint alleges deficiencies in the Lauder Plan's and defendant's policies and procedures, such as the failure to confirm authorization prior to making distributions, provide timely notice by telephone or email, or flag the multiple requests for distributions to accounts in different banks as suspicious. These deficiencies, the complaint argues, are breaches of the defendant's fiduciary duties.

The parties filed a notice of settlement on March 2nd. While the terms of the settlement are not public, this case laid the groundwork for questioning responsibility and remedies when data breaches and ERISA intersect.

Leventhal v. MandMarblestone Group, LLC

Similar to the Estee Lauder case, a plan participant (*and the plan sponsor*) filed a complaint in June 2018 seeking relief after approximately $400,000 was distributed from a 401(k) account. The participant sued both **MandMarbleStone Group, LLC ("MMG")**, as plan administrator, and **Nationwide Trust Company FSB ("Nationwide")**, as the plan custodian, after a cybercriminal obtained a copy of a participant's distribution form and used it to submit a series of fraudulent request for withdrawals.

In ruling on the defendants' motion to dismiss, the court determined that the complaint sufficiently pled that the administrator and the custodian were fiduciaries in connection with distributing the plan assets to participants and, as such, they could be held liable for breach of fiduciary duty in failing to enact prudent procedures and safeguards to protect the plan participants from security breaches. The court dismissed the state law claims.

MMG and Nationwide filed counterclaims against the plaintiffs, claiming that the plaintiffs' own carelessness with respect to its employees, computer systems, and policies allowed the cybercrime to occur. The counterclaim states that the plan sponsor is equally liable in its capacity as a named fiduciary of the plan and should be proportionally liable for the losses. On May 27, 2020, the court ruled that ERISA allows claims of contribution and indemnity.

While the court has not yet concluded that a fiduciary breach occurred, it notably held that the plaintiffs have, so far, sufficiently established that the administrator and custodian acted as fiduciaries in connection with the payment of distributions. Most courts have historically held that administrators and custodians do not act as fiduciaries, raising the question of whether protecting against cybercrime will change the relationship between ERISA plans and service providers.

Bartnett v. Abbott Laboratories et al.

Most recently, on April 3, 2020, a participant in the **Abbott Laboratories Stock Retirement Plan (the "Abbott Plan")** filed a lawsuit against Abbott Laboratories and Abbott Corporate Benefits, the individual designated as plan administrator, and Alight Solutions LLC, as the recordkeeper. Like the cases before, the complaint alleges that defendants failed to use the level of care and prudence required of an ERISA fiduciary when protecting plan assets. Specifically, the complaint alleges that the defendants breached their fiduciary duties by **(i)** failing to verify the participant's identity prior to making distributions, **(ii)** failing to establish safeguards to protect plan assets from unauthorized withdrawals, and **(iii)** failing to monitor other fiduciaries' distribution procedures and policies. Notably, just three days after the participant filed her complaint, the Department of Labor announced an investigation into Alight's processing of unauthorized distributions as a result of cybersecurity breaches.

According to the complaint, the hacker likely already had certain personal information about the participant prior to accessing the plan account, including the last four digits of the participant's social security number and date of birth. It's also likely the hacker had access to the participant's email. In December 2018, the hacker attempted to login to the participant's account by using the *"forgot password"* option and after entering the last four digits of the social security number and birthdate, the hacker was sent a one-time verification code via email, therefore gaining access to the participant's account. From there, the hacker changed the account password and added direct deposit information for a new bank account.

Two days later, someone called the Alight participant phone line from a number not associated with the participant's account and reported that a requested distribution did not go through. Alight did not allow the distribution to go through because it requires a seven-day waiting period between adding a new bank account and allowing distributions to the new account. Eight days later, someone again called the participant phone line and requested the distribution. Alight sent another verification code to the email address. The hacker was then able to distribute $245,000 to the new bank account.

In the complaint, the participant alleges that the defendants informed her about the addition of the new bank account and the distribution by regular mail. The participant argues that if the defendants had used email, she would have been able to question the security of her account and stop the transfer of the funds.

In June 2020, Abbott Laboratories and Alight filed competing motions to dismiss the complaint. Both motions disclaim any liability for fiduciary breaches in these circumstances and point the finger as to the other. In addition to determining whether the participant has stated a claim of fiduciary breach, the Northern District of Illinois will ultimately determine whether either Abbott or Alight (*or both*) have a fiduciary duty with respect to cybercrime, therefore commenting on fiduciary duties in regards to cybersecurity for plan sponsors and service providers.

Lessons Learned (thus far)

These cases accurately illustrate the complexities that arise in the aftermath of a data breach. While the Department of Labor has not yet issued guidance on how to address cybercrime against retirement plans or what types of protective measures should be in place, it is clear that plan sponsors and service providers must preemptively consider cybersecurity. Until the Department of Labor issues guidance, we must rely on the fiduciary duties of care, skill, prudence, and diligence.

But what exactly does that mean? What should plan sponsors and administrators consider? In light of the above cases, best practices could include:

- Both plan sponsors and service providers should review agreements to determine whether cybersecurity is discussed and the division of responsibilities.
- Plan sponsors should understand the cybersecurity policies and procedures the plan service providers have in place to protect participant personal information and plan assets.
- Plan sponsors should reserve the right to review the service provider's cybersecurity audits, like the Service Organization Control Reports.
- Both plan sponsors and service providers should encourage participants to regularly check plan accounts for any irregularities. Participants should have an easy method of contacting a service provider if concerned.

If case law and current events indicate anything, it's that issues of cybercrime are not going away any time soon. Plan sponsors and service providers both need to proactively (*and preemptively*) make cybersecurity a priority.

NIXON PEABODY

JENNY L. HOLMES
ASSOCIATE
NIXON PEABODY LLP
(585) 263-1494 | JHOLMES@NIXONPEABODY.COM

CERINI & ASSOCIATES LLP

CERTIFIED PUBLIC ACCOUNTANTS

Industries Served

Construction • Real Estate • Healthcare
Manufacturing • Technology
Professional Services • Consumer Services
Inbound Internal Businesses • Emerging Startups

Cerini & Associates, LLP
P: (631) 582-1600 | F: (631) 582-1714 | W: www.cerinicpa.com | 3340 Veterans Memorial Hwy., Bohemia, NY 11716