THE WAGNER LAW GROUP

LAW ALERT
June 4, 2020

Court Decision Highlights the Dangers of Cybersecurity Breaches for Both Plan Sponsors and Plan Service Providers

By Jordan Mamorsky

On May 27, 2020, the Eastern District of Pennsylvania, in *Leventhal v. MandMarblestone Group, LLC*, handed down a decision that highlights the dangers facing both plan sponsors and plan service providers when a cybersecurity breach results in money stolen from a participant's account. The court ruled that the TPA service provider, after being sued by the plan sponsor for the cybersecurity breach, may bring counterclaims against the plan sponsor for contribution and indemnity because the plan sponsor was alleged to be "careless" in its "computer/IT systems" and "employment policies" in permitting an employee and plan participant to work remotely without adequate safeguards to do so. The decision suggests a looming threat of security breaches and a resulting broad scope of fiduciary liability that can touch everyone involved in the running of a plan, regardless of traditional fiduciary titles.

The *Leventhal* decision comes against the backdrop of our current economic climate that, to be sure, raises the stakes for retirement plan cybersecurity. Plan sponsors are operating in a novel environment, where more employees are working remotely than ever before, many of their participants might be furloughed or unemployed, and the CARES Act makes it more accessible and attractive for employees to withdraw from their 401(k) plans. The collision of these factors (and others in our current stay-at-home economy) make securing participant retirement accounts all the more vital. The Leventhal case highlights the importance of protecting against cybersecurity breaches in the midst of these unusual times.

Service Providers Sued, Alleged to be Fiduciaries

As a starting point, last May the Eastern District of Pennsylvania first ruled in this case that the TPA, MandMarblestone Group ("MMG"), and the plan's custodian, Nationwide, were ERISA fiduciaries in connection with distributing plan assets to participants. The court then reasoned that Nationwide and MMG could be held liable for breach of fiduciary duty in failing to enact prudent procedures and safeguards to protect the plan and participants from cybercriminals who obtained a copy of a participant's distribution form and used it submit a series of requests for fraudulent withdrawals totaling more than $400,000.

As ERISA fiduciaries, the court concluded that the TPA and custodian failed to act with the requisite prudence and diligence under ERISA Section 404 when they observed the "peculiar nature" and "high frequency" of the withdrawal requests that were to be distributed to a new bank account and also failed to implement "typical" procedures and safeguards to notify participants and/or verify the requests.

The Service Providers Fight Back Against the Plan Sponsor

Considering that this was an unusual finding - particularly in holding a plan custodian liable for breach of fiduciary duty — Nationwide and MMG fought back, but with divergent paths. In response to the court's finding, MMG counterclaimed against plaintiffs that "Plaintiffs' ***own carelessness*** with respect to their employees and their

computer/IT systems and policies, including their decision to permit [the plan participant] to work remotely from Texas and use her personal e-mail for official employment duties, permitted the cyber-fraud or other criminal fraud to occur." MMG's counterclaim hung its hat on the concept that, if the TPA was indeed a fiduciary, then plaintiffs as the named fiduciary, trustees, and plan sponsor, were liable for co-fiduciary contribution and indemnification for any losses incurred because of their carelessness.

Separately, Nationwide, the plan's custodian, pushed back against the plaintiffs' breach of fiduciary duty allegations, but instead of making a counterclaim against the plaintiffs, it asserted (i) affirmative defenses (with MMG) that sought equitable contribution for the portion of loss allegedly caused by plaintiffs; and (ii) a third party complaint against the actual criminals who stole the money from the plan. The court denied MMG and Nationwide's affirmative defenses because it reasoned their joint and several liability owed to the plan, as ERISA fiduciaries, could not be limited through the assertion of affirmative defenses. It also denied Nationwide's third party complaint against the perpetrators of the fraud because Nationwide did not plead any facts that they were fiduciaries or parties in interest to the plan, a necessary requisite for liability under ERISA.

The Court Allows a Contribution Counter Claim Against the Plan Sponsor

On MMG's counterclaim, the court made important conclusions of law that will have significant effects for this evolving area of ERISA fiduciary law. The noteworthy aspect of the court's decision was that it permitted MMG to seek co-fiduciary contribution against the plaintiffs based primarily upon the principles of fiduciary contribution in trust law and permitted Nationwide to amend its answer to the complaint to bring a counterclaim for contribution and indemnification.

The practical and legal implications of this finding are meaningful. First, allowing for co-fiduciary contribution in response to a cybersecurity breach of fiduciary claim will likely result in defendant service providers pursuing this counterclaim in the Second Circuit (New York, Connecticut), Third Circuit (New Jersey, Pennsylvania, Delaware), and Seventh Circuit (Illinois, Wisconsin, Indiana). While the Third Circuit has not joined the Second and Seventh Circuits in explicitly permitting co-fiduciary contribution, this is another decision that adds to a growing number of cases there that support that premise in the jurisdiction. Other circuit courts such as the Eighth Circuit have rejected contribution counterclaims under ERISA.

Second, the Eastern District of Pennsylvania made a compelling argument for co-fiduciary contribution rooted in the common law of trusts - a connection the Supreme Court has often made in its decisions analyzing the scope of ERISA's fiduciary protections. Courts favoring co-fiduciary contribution have adopted this reasoning before and, in the future, other courts might also latch onto this logic, that where "two trustees are liable to the beneficiary of a trust, each of them is entitled to contribution from the other." See Restatement (Second) of Trusts § 258 (1959).

What Plan Sponsors and Plan Service Providers Should be Doing

Practically, the court's decision in favor of contribution and indemnification should only encourage more plan sponsors to carefully study their plan documents and service provider contracts to ensure they cover all possible circumstances, including cybersecurity breaches. We discuss action steps plan sponsors should consider taking in this prior Alert. It is essential that the employer, in its capacity as a fiduciary to its retirement plan, have a clear conception of who will be responsible (it or a service provider) in the event of a cybersecurity breach such as occurred in *Leventhal*. A smartly worded plan document and service provider agreement could assist towards that end.

From a broader perspective, the decision should serve as a warning for plan sponsors who might not believe they have liability for cybersecurity breaches when they delegate that responsibility to a TPA. This fact set, particularly in light of the reality of today's stay-at-home economy, should motivate plan sponsors to revisit their current systems and procedures to protect against cybersecurity breaches, as well as the procedures employed by their

service providers to verify participant identities. When such procedures are not prudent or reasonable and can be easily foiled by cybercriminals, the consequences, as demonstrated by *Leventhal*, could result in all plan related actors holding the proverbial bag as co-fiduciaries.

Before an incident arises, plan sponsors and service providers should proactively address issues of cybersecurity in more detail with their ERISA counsel.

www.wagnerlawgroup.com

@wagner-law-group
fb.com/WagnerLawGroup

Boston:
99 Summer Street, 13th Floor
Boston, MA 02110
Tel: (617) 357-5200

@wagnerlawgroup
@wagnerlawgroup

Boynton Beach:
1880 N. Congress Avenue, Suite 200
Boynton Beach, FL 33426
Tel: (561) 293-3590

Chicago:
190 South LaSalle Street, Suite 2100
Chicago, IL 60603
Tel: (847) 990-9034

Lincoln, MA:
55 Old Bedford Road, Suite 303
Lincoln, MA 01773
Tel: (617) 532-8080

New York:
200 Park Avenue, Suite 1700
New York, NY 10166
Tel: (212) 338-5159

San Diego:
8677 Villa La Jolla Drive, Suite 888
San Diego, CA 92037
Tel: (619) 232-8702

San Francisco:
315 Montgomery Street, Suite 900
San Francisco, CA 94104
Tel: (415) 625-0002

St. Louis:
1099 Milwaukee Street, Suite 140
St. Louis, MO 63122
Tel: (314) 236-0065

Tampa:
101 East Kennedy Boulevard, Suite 2140
Tampa, FL 33602
Tel: (813) 603-2959

Washington, D.C.:
800 Connecticut Avenue, N.W., Suite 810
Washington, D.C. 20006
Tel: (202) 969-2800