WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

April 2, 2021

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Kate A. Jarrett
313.327.3127 (direct)
Kate.Jarrett@wilsonelser.com

VIA: Email Only

Attorney General Gordon MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
(603) 271-3643
DOJ-CPB@doj.nh.gov

Re: Netgain Cybersecurity Incident
Client: PKF O'Connor Davies ("PKFOD")
File No.: 11077.00106

Dear Attorney General MacDonald:

We represent PKF O'Connor Davies ("PKFOD") an accounting and advising firm with regard to a cybersecurity incident that impacted its third party vendor, Netgain Technology, LLC ("Netgain"). PKFOD is headquartered in New York, with a presence in New Jersey, Connecticut, Maryland and Rhode Island.

1. **Nature of the incident.**

On December 3, 2020, Netgain first advised PKFOD that Netgain was the victim of a cybersecurity incident that impacted Netgain's systems. Netgain's investigation revealed that the threat actor initially gained access to PKFOD's hosted environment on November 8, 2020. Between November 10 and November 23, 2020, the threat actor deployed various tools associated with the archiving and exfiltration of data. On December 3, 2020, according to Netgain, the threat actor began encrypting files hosted by Netgain.

On December 10, 2020, Netgain notified PKFOD that the Threat Actor successfully exfiltrated files related to PKFOD. Netgain provided PKFOD with a screenshot of the files accessible by the threat actor. PKFOD reviewed the compromised files and discovered that the files contained personal information, including name, Social Security Number, financial account information, and/or tax documents.

2. **Number of New Hampshire residents affected.**

PKFOD discovered that four (4) residents of New Hampshire were impacted by the Netgain cybersecurity incident. Notification letters were sent to these individuals between December 22, 2020 and January 29, 2021. A sample notice letter that was sent to each impacted individual is included as **Exhibit A**.

3. Steps taken.

The remediation measures undertaken by Netgain include deploying threat-detecting tools across its environment and rotating all user credentials. Netgain also ran scripts to ensure that all backups were clean prior to restoring any infected systems. PKFOD provided complimentary credit monitoring to the impacted individuals for at least twelve (12) months.

4. Contact information.

PKFOD remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

December 24, 2020

Dear [redacted] Fund Investor:

We write to advise you of a cybersecurity incident ("Incident"), that may have resulted in the compromise of your personal information.

Notice of Cybersecurity Incident

We recently learned that the third-party host for our data, Netgain Technology, LLC ("Netgain"), was the subject of the Incident, which may have resulted in the compromise of your personal information. [redacted] and PKF O'Connor Davies LLP ("PKFOD"), take the privacy and security of our customers' data very seriously, and we regret having to advise you of this Incident. We are taking this opportunity to provide you with important information we have received from Netgain, including steps taken by Netgain to mitigate the risk of future threats and exposure of customer data, steps PKFOD and [redacted] have taken to protect against possible misuse of your personal information, and steps you may take to protect against possible misuse of your personal information.

Who is Netgain and Why Did They Have Your Information?

Netgain is a Cloud storage and data hosting provider headquartered in St. Cloud, Minnesota. PKFOD utilizes Netgain's hosting services to store data of investors in The Weiller Value Fund. At all times, Netgain has assured PKFOD that such data is stored in specially designated data repositories that are both secure and segregated from other Netgain customers.

What Happened?

On December 3, 2020, Netgain first advised PKFOD that Netgain was the victim of a cybersecurity incident that impacted Netgain's systems. PKFOD in turn verbally advised [redacted] on December 13, 2020 of the Incident and formally notified [redacted] on December 20, 2020. To contain the impact and possible spread of infection, Netgain promptly took its systems offline. Netgain engaged leading cybersecurity professionals to assist with the remediation efforts and to conduct a forensics investigation to determine the nature and scope of the Incident. We understand that that investigation is ongoing although the vulnerability has been patched and all data has been safely restored.

We have since learned from Netgain that the Incident in question involved a ransomware attack. We understand that Netgain paid an undisclosed amount to the threat actor. Netgain's investigation revealed that the threat actor initially gained access to PKFOD's hosted environment on November 8, 2020. Between November 10 and November 23,

2020, the threat actor deployed various tools associated with the archiving and exfiltration of data, On December 3, 2020, the threat actor began encrypting files hosted by Netgain.

What Information was Involved?

The impacted files may contain your personal information, including your name, address, phone number, Social Security Number, financial account information, passport information, and/or tax documents.

Netgain has informed us that it is continuously monitoring the Dark Web to determine if any PKFOD client data involved in this Incident has been published by the threat actor. There is currently no indication that any of the data accessible has been published or used to commit fraud or identity theft.

What Steps Have PKFOD and [redacted] Taken in Response to this Incident?

The remediation measures undertaken by Netgain include deploying threat-detecting tools across its environment and rotating all user credentials. Netgain also ran scripts to ensure that all backups were clean prior to restoring any infected systems. At this time, Netgain is bringing its systems online once they have been deemed to be free of infection or any lingering malware.

In addition to the security team retained by Netgain, PKFOD hired an independent, third-party team of cybersecurity experts to verify the findings of Netgain's investigation and to ensure their systems are safe and secure. We are now taking the appropriate steps to notify those impacted by the Incident.

Netgain, PKFOD, and their teams of experts have been working around the clock since the Incident. Our shared goal is to provide accurate and transparent information to those impacted and to assist as necessary to limit any harm caused by this Incident.

What Can You Do to Protect Yourself?

While we are presently unaware of any misuse of your information as a result of this incident, in an effort to help relieve any concerns as a consequence of this incident, we are providing you with complimentary services to help protect your identity, whether or not it was affected. In response to the incident, we are offering you services provided by **CyberScout,** a company specializing in fraud assistance and remediation services.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring*** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy.

Activation codes and a contact telephone number will be sent as soon as available from CyberScout.

We encourage you to remain vigilant in response to this Incident and to enroll in the complimentary credit monitoring services provided to you. For those of you who have access to the PKFOD investor portal, we encourage you to update your password.

The protection of your information is our top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to contact us at eiglicki@pkfod.com.

Sincerely,

PKF O'Connor Davies, LLP

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of

identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.