17450

GLOBAL ENDOWMENT MANAGEMENT

August 4, 2020

Dear Investor,

We are writing to inform you that on July 16, 2020, we were notified that Global Endowment Management, LP ("GEM") client data was impacted in a ransomware attack suffered on or about May 17, 2020 by a third-party vendor used by SEI Global Fund Services ("SEI"), our third-party fund administrator, that manages the SEI Investor dashboard portal. The third-party vendor affected by the attack, M.J. Brunner, Inc. ("M.J. Brunner"), provides direct marketing, public relations, digital and mobile design across multiple industries, and assists SEI with website and application development and maintenance. SEI is working with M.J. Brunner, the FBI and several external cybersecurity experts to investigate this matter. We continue to receive updates from SEI, and will continue to follow up to gather more information as it becomes available. The information below summarizes our current understanding. Since this remains a fluid situation, the information below may change.

SEI informed us that this attack resulted in the unauthorized public disclosure of certain client data. We do not know the full extent of the data that has been compromised, but we believe that anyone using the SEI Investor Dashboard portal in relation to one of our funds was affected, and feel it is prudent to notify you of the potential impact. We believe this to be a broad corporate attack and not specific to SEI, our firm, or our clients. SEI believes that the attackers have obtained certain data elements relating to user profiles and a subset of documents that were available on the Investor Dashboard. **Please note that neither ours nor SEI's networks were compromised or infiltrated in the attack.**

To the best of SEI's knowledge, the following types of data were compromised, and may now have been publicly exposed:

SEI Investor Dashboard User Information:

- Name of the SEI Investor Dashboard portal user
- Investor name and SEI account ID (an internal code used by SEI only)
- Email address
- Phone number (used for registering the SEI online access)
- SEI Portal Username
- Association with Global Endowment Management, LP ("GEM") as either an investor or an interested party

Investor Documents:

- A copy of a GEM Fund investor statements issued through July 2016 containing investor name and holdings information
- A copy of K1s issued by a GEM Fund through the 2015 calendar tax year containing investor name, social security number/employer identification number
- A copy of your subscription document for each GEM Fund submitted through July 2016 containing information you provided during the application process including investor name, social security number/employer identification number and wiring instruction details

At this juncture, SEI is not able to determine whether all the investor data fields described above were compromised for some or all investors in our funds. However, in the interest of maximum security, we are moving forward as if the attackers obtained all the data from each field listed above for every investor who utilized the SEI Investor Dashboard. Based on the information currently available, SEI believes that user login credentials (passwords, security questions, etc.) were **NOT** compromised by the attack. Additionally, SEI employs two-factor authentication. We are continuing to communicate with SEI, and we will alert you with relevant material updates that we receive from SEI.

SEI remains dedicated to keeping your personal information safe. They have notified law enforcement and are continuing to investigate this matter. We suggest that you remain particularly vigilant to potential phishing attempts by email or phone. Other than the one-time pin, SEI and GEM will not email or call you with any links to reset your password. You will be prompted to reset your password on your next login attempt to the SEI Investor Dashboard.

Please review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud" for further information on steps you can take to protect your personal information, and how to receive free credit monitoring for two years.

We are continuing to work with SEI to investigate this matter, and we will keep you apprised of additional information as it becomes available. SEI is available to answer any questions that you may have, and we are available to speak to you about this as well. Please feel free to contact Rich Abraham at rabraham@globalendowment.com with any questions or to setup a discussion with SEI.

Best regards,

Rich Abraham
Chief Financial Officer/Chief Compliance Officer
Global Endowment Management, LP

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

We recommend you be on the alert for suspicious activity related to your financial accounts. **Be vigilant of any suspicious activity or unauthorized attempts to log on to your accounts, phishing emails, and any other attempts to access your information.** In addition, we would like to take this opportunity to remind our investors of best practices they can employ to avoid being victimized by hackers. We believe it is prudent to take all cybersecurity precautions that you can, such as exercising good password hygiene and network security. Stolen personal data provides hackers with the opportunity to conduct social engineering, phishing and other online email frauds against you and others. **When hackers have information about you, it is easier for them to create authentic looking communications in an effort to dupe you or others into believing their fraudulent communications are authentic.** In this regard, we suggest the following:

- Do not click on a link or open an attachment from a person that you do not know
- Be suspicious of links and attachments sent to you, even from someone you know
- Be suspicious of any email that asks you to click and provide login credentials
- Never provide wire information or accept wire information without confirming the request is authentic
- Never enter sensitive information in a pop-up window
- Beware of social engineering and fraudulent phone calls
- Employ phishing protection best practices and take any other measures you believe are necessary to protect your data

Complimentary Credit Monitoring Services

To help alleviate concerns related to this event, SEI is offering a complimentary two-year membership of Experian's® IdentityWorks℠ . This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

Membership activation for U.S. domiciled persons:

- Ensure that you **enroll by:** October 31, 2020 (your code will not work after this date)
- **Visit** https://www.experianidworks.com/3bcredit ,the Experian IdentityWorks website to enroll
    - Provide your **activation code: SFSPB4XBT (Please keep this code confidential as it is specific to GEM)**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **October 31, 2020**. Be prepared to provide engagement number **DB21589** as proof of eligibility for the identity restoration services by Experian. We are also working with SEI to understand what coverage will be available for non-U.S. domiciled persons. We will provide more information about this service as SEI provides it to us.

Membership activation for non-U.S. individuals*:

- Ensure that you **enroll by**: October 31, 2020 (your code will not work after this date.)
- Visit www.globalidworks.com/identity1, the Experian IdentityWorks website to enroll
    - Provide your **activation code: DTXXXVDJK (Please keep this code confidential as it is specific to GEM)**

If you have questions about the product, or need assistance with identity restoration, please contact Experian's customer care team at globalidworks@experian.com .

* The non-U.S. personal information monitoring is available in the following countries: Australia, Brazil, Canada, Germany, Hong Kong, India, Ireland, Italy, Mexico, the Netherlands, New Zealand, Poland, Singapore, Spain and the UK. If you are a non-U.S. individual in a country other than those listed, please contact us directly.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the major credit bureaus listed below to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the major credit bureaus listed below if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. Fees vary based on where you live,

but commonly range from $3 to $15. To find out more on how to place a security freeze, obtain a credit report, or fraud alert, you can use the following contact information:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General.

For North Carolina Residents: The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov.

For Massachusetts Residents: You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.