CADWALADER

Cadwalader, Wickersham & Taft LLP
200 Liberty Street, New York, NY 10281
Tel +1 212 504 6000 Fax +1 212 504 6666
www.cadwalader.com

January 13, 2021

VIA EMAIL

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of data breach

Dear Mr. Attorney General:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20, we are writing on behalf of our client, ACRES Capital Debt Opportunity Fund L.P. (the "Fund") to notify you of a data security incident. The incident involve a single Fund client who is a New Hampshire resident.

The incident involved a ransomware attack at Netgain Technology, LLC ("Netgain"), a technology subcontractor of PKF O'Connor Davies ("PKF" or the "Administrator"). Netgain is a cloud storage and data hosting provider; the Administrator utilizes Netgain's hosting services to store certain data belonging to the Fund's clients.

The Fund was first notified of the incident on December 13, 2020 and immediately commenced an investigation. Based on that investigation, the Fund understands that the ransomware attack occurred at Netgain on or about November 8, 2020. Between November 10th and November 23rd, the ransomware perpetrator utilized various tools enabling the taking of data, and on December 3rd, the perpetrator began encrypting customer files at Netgain. Netgain became aware of the incident on December 3rd, and promptly took its systems offline. Netgain engaged cybersecurity professionals to assist with the remediation efforts and to conduct a forensics investigation to determine the nature and scope of the incident. Netgain advised the Administrator of the incident on December 3rd.

Based on Netgain's investigation, the Fund believes the attacker had access to certain investor information stored on Netgain's system. The information accessed by the attacker included: first and last name, full address, bank account information, Social Security Numbers, and/or tax

Scott Cammarn Tel (704) 348-5363 scott.cammarn@cwt.com

documents (including W-9s). At this time, the Fund is not aware of any misuse of or fraud associated with individual investors' personal information.

The Fund will notify the relevant New Hampshire resident of this incident through its investor portal, which the resident has previously agreed to use for purposes of receiving notifications relating its investment in the Fund. The Fund is providing this individual with an offer for complimentary credit monitoring and identity protection services through CyberScout. An individual can enroll in the CyberScout services on the CyberScout website or phone number listed in the notice.

Enclosed for your reference is a copy of the notice that will be electronically distributed to the affected investor on January 13, 2021.

Please do not hesitate to contact me at (704) 348-5363 if you have any questions. I can also be reached at Cadwalader, Wickersham & Taft, LLP, 227 W. Trade St., Charlotte, NC 28202 or at scott.cammarn@cwt.com.

Sincerely,

Scott Cammarn
Partner

Attachment

ACRES Capital, LLC
865 Merrick Ave., Suite 200S
Westbury, NY 11590

COPY

[Recipient Name]
[Recipient Address]

January 13, 2021

Re: Notice of data breach relating to your investment in ACRES Capital Debt Opportunity Fund L.P. (the "Fund")

Dear [Recipient],

We are writing to notify you regarding an information security breach at a subcontractor for the Fund's Administrator, PKF O'Connor Davies ("PKF" or the "Administrator"). The breach involved a ransomware attack at Netgain Technology, LLC ("Netgain"), a technology subcontractor of PKF. Netgain is a Cloud storage and data hosting provider headquartered in St. Cloud, Minnesota; the Administrator utilizes Netgain's hosting services to store certain data of the Fund's clients. We currently have no reason to believe your personal data has been stolen or misappropriated. Nonetheless, we would like to share information we received regarding the incident so you can take steps to protect yourself.

The Incident

The Fund was first notified of the incident on December 13, 2020 and immediately commenced an investigation. Based on that investigation, we understand that the ransomware attack occurred at Netgain on or about November 8, 2020. Between November 10th and November 23rd, the ransomware perpetrator utilized various tools enabling the taking of data, and on December 3rd, the perpetrator began encrypting files at Netgain. Netgain became aware of the incident on December 3rd, and promptly took its systems offline. Netgain engaged 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 Netgain has adopted enhanced security and threat detection measures to prevent a recurrence, and has brought its systems online after having determined its systems to be free of infection or any lingering malware. We understand the ransomware perpetrator has agreed in principle to destroy any Netgain information in its possession.

Netgain advised the Administrator of the incident on December 3rd. Following Netgain's investigation, Netgain provided the Administrator with a screenshot of files that Netgain believes the perpetrator may have had access to. These files include certain data regarding the Fund and the Fund's investors. This data may include personal information contained in the Fund's Subscription Documents (which may contain an investor's name, address, bank account information, Social Security Numbers, and/or tax documents including W-9s).

At this time, we are not aware of any misuse of or fraud associated with individual investors' personal information. We understand that the cybersecurity professionals retained by Netgain have been continuously monitoring the Dark Web for any such information. To date, there is no indication that any data accessible by the perpetrator has been published on the Dark Web or elsewhere.

Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected investors about the incident, and about tools you can use to protect yourself going forward. The confidentiality, privacy and security of personal information within our care is among ACRES's highest priorities. We have instructed both PKF and Netgain to destroy all information in their possession relating to the Fund's investors and have taken and continue to take steps to improve security and better protect against similar incidents in the future.

What Information Was Involved?

The impacted files may contain your personal information, including your name, address, bank account information, Social Security Numbers, and/or tax documents including W-9s. To date, there appears to be no indication that any data accessible by the perpetrator has been used to commit fraud or identity theft.

What Are We Doing?

ACRES has completed its investigation, which commenced as soon as it was informed of the incident at Netgain on December 13th. We understand that the Administrator began its investigation on December 10th once Netgain advised the Administrator that its files may have been impacted. Although Netgain had previously assured the Administrator that the Fund's data is stored in specially designated secure data repositories, the Administrator hired an independent, third-party team of cybersecurity experts to verify the findings of Netgain's investigation and ensure its systems are safe and secure.

What You Can Do

ACRES is not aware currently of any misuse of your personal information. Nonetheless, given the nature of the Incident, ACRES wishes to notify you out of an abundance of caution. As an added precaution, ACRES is offering you access to 12 months of credit monitoring and identity protection services through CyberScout at no cost to you. Enrolling in this service will not affect your credit score. If you enroll, CyberScout will provide you with same-day alerts when changes occur to your Experian credit file. Additionally, CyberScout will monitor the dark web and you will receive an alert if your personally identifiable information is found online. Finally, CyberScout will provide proactive fraud assistance to help with any questions you have at this time or in the event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy.

If you would like to receive monitoring services you must enroll with CyberScout by April 13, 2021.

To enroll in CyberScout Credit Monitoring services:

1. Log on to https://cs4protect.com and follow the instructions.

2. When prompted please provide the following unique code: [redacted]

3. Once registered, you can access monitoring services by selecting the "Use Now" button to authenticate your identity and activate your services. All of the monitoring services described above are accessible at https://cs4protect.com.

4. If you have questions while registering, please call CyberScout at 1-800-405-6108 to reach a live representative.

Credit Reports: In addition to enrolling in the above offered services, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three 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 three major credit bureaus directly to request a free copy of your credit report. Checking your credit reports periodically can help you spot problems and address them quickly.

Security Freeze: You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved without your express authorization. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have up to three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have up to three (3) business days after receiving your request to remove the security freeze.

Fraud Alerts: As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a

victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-alerts

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You may also wish to review the tips provided by the Federal Trade Commission (the "FTC") on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

If you suspect you have been the victim of identity theft, you should contact law enforcement.

For More Information

ACRES takes the privacy and security of its investors quite seriously, and deeply regrets any inconvenience the incident at Netgain has caused to you and the Fund. As stated above, despite the incident, ACRES is not aware that any of your personal information has been misused. Nonetheless, we remain committed to provide transparent communications as we learn more and work to fully recover from this unfortunate event. If you have questions regarding this incident, please call (516) 206-1357, Monday – Friday between the hours of 9:00 am and 6:00 pm (Eastern).

Sincerely,

Andrew Fentress
Managing Partner