<<Return Mail Address>>

<< First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>
United States

<<Date>>

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

On or around May 13, 2023, Blockchain Capital, LLC ("Blockchain Capital") became aware of suspicious activity related to its computer systems. In response, Blockchain Capital promptly launched an investigation. As a result of this investigation, Blockchain Capital determined that an unauthorized third party may have accessed or acquired documents containing personal information related to certain of its limited partners. On or around June 2, 2023, Blockchain Capital identified that these impacted documents contained your personal information. Although at this time there is no indication that your personal information has been misused in relation to this event, we are providing you with information about the event, our response, and steps you may take to help protect against the possibility of identity theft and fraud.

What Happened? On or around May 13, 2023, Blockchain Capital became aware of suspicious activity on our computer systems. We swiftly launched a response to secure our systems and worked with cybersecurity specialists to investigate the nature and scope of the activity. After identifying the means and method of the event, Blockchain Capital undertook a comprehensive, manual review of the documents impacted by the incident. Through this review, Blockchain Capital identified that your personal information was contained in the impacted documents.

What Information Was Involved? The impacted documents included your name, postal address, email address, telephone number, and Social Security number. At this time, we do not have any evidence that impacted individuals have experienced fraud or misuse as a result of the event. Although at this time there is no indication that your personal information has been misused in relation to this event, Blockchain Capital is providing this notice as a precaution.

What We Are Doing. Information security is among Blockchain Capital's highest priorities, and we take this incident very seriously. Upon discovering this suspicious activity, we immediately took steps to review and reinforce the security of our systems. We have reviewed existing security policies and have implemented additional cybersecurity measures in an effort to further protect against similar incidents moving forward. Specifically, we have reviewed and updated our multi-factor authentication protocols and are working on further enhancing our authentication controls, including by developing additional mechanisms for restricting access to personal information. We have also reported this event to law enforcement. However, please note that this notice has not been delayed as a result of a law enforcement investigation. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

As an added precaution, we are offering you a complimentary twenty-four (24) month membership to Experian IdentityWorks℠ at no cost to you. We encourage you to enroll in these services as we are not able to do so on your behalf. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [Activation Code]

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 [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the identity restoration services provided by Experian.

What You Can Do. We regret any inconvenience or concern this event may cause. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached "Additional Resources" document. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While Blockchain Capital will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please contact Jason Di Piazza, Head of Capital Formation, at 415-630-2370. You may also write to Blockchain Capital at 440 Pacific Ave. San Francisco, CA 94133.

Sincerely,

[Signature]

Jason Di Piazza
Blockchain Capital, LLC

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

A credit card is **not** required for enrollment in Experian IdentityWorks.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) month membership.

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditregort.com. by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit

account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
http://www.marylandattorneygeneral.gov

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For residents of the District of Columbia: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:

Office of the Attorney General for the District of Columbia
Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
(202) 442-9828
https://oag.dc.gov/

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office
Office of the Attorney General
The Capitol

Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/

New York Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
844-891-1786
https://its.ny.gov/

For Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub, or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.