Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: July 29, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

April 29, 2026

NOTICE OF DATA BREACH

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

The safety and privacy of our investors' data is of paramount importance to us. For this reason, as a precautionary measure, we are writing to let you know about a data security incident that likely involved your personal information.

WHAT HAPPENED:

On February 16, 2026, Mudita Venture Partners was the victim of a targeted cyber-attack in which an unauthorized third party gained access to certain personal information in the company's infrastructure.

Mudita became aware of the security incident on February 18, 2026, when an external party notified us of fraudulent activity. We immediately launched an investigation and engaged a cybersecurity firm to perform a forensic investigation and threat hunt. Remediation of the compromised account was completed the same day, including credential resets, revocation of all active sessions, and a review of mailbox rules and configurations to remove any persistence mechanisms established by the threat actor.

On April 13, 2026, Mudita became aware that certain documents were accessed during the cyber-attack. Steps have been, and are currently being, taken to contain and remediate any potential harm related to the information in the documents accessed. Law enforcement has not delayed this notification.

WHAT INFORMATION WAS INVOLVED:

On April 13, 2026, it was determined with reasonable certainty that certain investor data was accessed. As of today, we are aware that you are included in a group whose potentially accessed data included the following categories of information:

- **Personal and tax identification information:** Name, home address, Social Security number (SSN) or Employer Identification Number (EIN), and investment amount. For some individuals, email addresses and signatures were also exposed.

We have not received any information indicating that the information described above has been disseminated to persons aside from the unauthorized actor who accessed the data.

WHAT WE ARE DOING:

Upon becoming aware of the attack, Mudita immediately launched an investigation and engaged a cybersecurity firm to perform a comprehensive forensic investigation and threat hunt. We took immediate action to secure the compromised account, including credential resets, session revocation, and removal of any persistence mechanisms. We have also taken additional measures to prevent further incidents, including implementing phishing-resistant multi-factor authentication, Endpoint Detection and Response (EDR), identity and cloud protection, and continuous monitoring and alerting across our systems.

Mudita takes this cyber-attack very seriously. While this letter serves as notification of the cyber incident, we and our experts are continuing to diligently assess the situation and will provide an update should we obtain any additional information regarding the compromise of your personal information. We have also previously communicated with our Investor Community regarding security awareness, including guidance on verifying the authenticity of any communications purporting to come from Mudita.

WHAT YOU CAN DO:

Given the nature of this incident, we suggest that you take precautionary measures, such as changing the passwords to your financial accounts and answers to your security questions, and remain vigilant by monitoring accounts and obtaining free credit reports.

In addition, Mudita is offering identity theft protection services through IDX at no cost to you. IDX identity protection services include 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that these services are for individuals only. Entities and Businesses are not covered by the enrollment code provided above.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-788-9712, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time, excluding holidays. Please note the deadline to enroll is July 29, 2026.

For more information, please see the enclosure entitled "Steps You Can Take to Further Protect Your Information." We value your privacy and deeply regret that this incident occurred. We will notify you if there are any significant developments.

Sincerely,

Ruchira Dasgupta
Chief Operating Officer
(607) 342-8569

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. For further information about preventing identity theft, or to register a concern, you may also contact the Federal Trade Commission (FTC) at IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). The FTC's physical address is: 600 Pennsylvania Avenue NW, Washington, DC 20580. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. You may also contact your local police to exercise your right to obtain a police report.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

Access the form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(888) 378-4329	(888) 397-3742	(877) 322-8228
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	2 Baldwin Place, P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

OTHER IMPORTANT INFORMATION

Security Freeze

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately

place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.