SUTTER HILL VENTURES
755 PAGE MILL ROAD
SUITE A-200
PALO ALTO, CALIFORNIA 94304-1005

PHONE (650) 493-5600
FAX (650) 858-1854

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear **<<first_name>>**,

We are writing to inform you of a security incident involving your personal information held by Sutter Hill Management Company, LLC ("Sutter Hill"). We sincerely regret any concern this may cause you and encourage you to take the steps discussed below to help protect yourself.

What Happened?

We recently learned that an unauthorized actor gained access to some of Sutter Hill's computer systems and data on February 24, 2024. Upon becoming aware of the issue, we promptly began an investigation and determined that the unauthorized actor was able to take certain data from our systems. Based on our investigation, you were one of the individuals whose personal information was affected by this incident.

What Information Was Involved?

The personal information affected by the incident may have included your social security number, government-issued identification, and health insurance information. Please note that, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address this incident promptly, including retaining an independent forensic investigation firm to assist us in our investigation of and response to this incident. Additionally, we have worked closely with external experts to implement enhanced security measures designed to help prevent this type of incident from reoccurring in the future.

To help protect your identity, we are offering twenty-four (24) months of complimentary identity protection services from a leading identity monitoring services company (Kroll). These services can help detect possible misuse of your personal information and provide you with identity protection support focused on prompt identification and resolution of identity theft.

What You Can Do

Although we are not aware of any misuse of any information arising out of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering twenty-four (24) months of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that to obtain these services, you must complete the enrollment process by <<b2b_text_6 (ActivationDeadline)>>.
- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of

the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.

- **Contacting Tax Agencies.** You can contact the IRS hotline at 800-908-4490 or visit https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers. You can also establish or request a new Identity Protection PIN ("IP PIN"), which provides an additional layer of identity verification when filing a federal tax return with the IRS. Details on how to establish or request a new IP PIN can be found at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. Answers to common questions about IP PINs can be found at https://www.irs.gov/identity-theft-fraud-scams/frequently-asked-questions-about-the-identity-protection-personal-identification-number-ip-pin.

  You can also file an IRS Form 14039 "Identity Theft Affidavit" with the IRS if you believe that someone has attempted to file a fraudulent tax return in your name. You can complete and submit Form 14039 electronically at https://apps.irs.gov/app/digital-mailroom/dmaf/f14039/, or you can print and mail/fax a paper copy of Form 14039 using the PDF version available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. There may also be similar resources and forms to file for individual states, so we recommend that you check directly with your state tax authority for more information. For example, California taxpayers can call the California Department of Tax and Fee Administration at 800-400-7115 or visit https://www.cdtfa.ca.gov/contact.htm for more contact options. A listing of other state tax agencies' websites is available at http://www.taxadmin.org/state-tax-agencies.

- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer/health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan.

- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact me at (650) 493-5600 between the hours of 9:00AM – 5:00PM Pacific time, Monday through Friday or via email at chris@shv.com. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Chris Basso

Managing Director/ CFO

Activating and Using Your Complimentary Identity Monitoring

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report
Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

Bank Account Alerts
This service monitors to see if an Activated Participant's Social Security number (SSN) or personal information has been used to open new bank accounts or make changes to current accounts. This service pulls from a large network of financial institutions, including the top 10 regional banks and credit unions. If new inquiries, account openings or changes to existing accounts are detected, this service generates an email alert to notify the Activated Participant so he or she can review the information and determine whether the action was authorized or could be the result of identity theft.

Participating financial institutions are subject to change.

Minor Identity Monitoring
Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should 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 Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from 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.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Information About Medical Identity Theft: Patients who pay for medical services can regularly review the explanation of benefits (EOB) statements that they receive from their health insurers or health plans. If they identify services listed on the EOB that were not received, they should immediately contact the health plan. For more information about protecting yourself from the Department of Health and Human Services, please visit https://oig.hhs.gov/fraud/medical-id-theft.

Security Freezes and Fraud Alerts: You have a 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 in your name without your consent. 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241, Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)
General Contact:
P.O. Box 2104, Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9556, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact, Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
800-916-8800