GUARDANT™

505 Penobscot Drive
Redwood City, CA 94063

October 22, 2018

Notice of Data Breach

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Dear Sir or Madame:

Pursuant to N.H. Rev. Stat. § 359-C:20, we are writing to inform you of an incident that may have resulted in unauthorized access to personal information involving a small number of Massachusetts residents.

What Happened
On August 23, 2018, Guardant Health learned that certain company shared email accounts may have been accessed by an unauthorized actor. We promptly took steps to stop the unauthorized access and began an investigation with a leading cyber forensics firm to help us determine what data may have been accessed as a result of this incident. In the course of our investigation, we determined that there may have been access to personal information in the email messages on these accounts during a period of time between February 24 and August 14, 2018. On September 13, 2018, our investigation was able to determine what information may have been breached and what individuals may have been impacted. Based on these results, we are providing notice to affected individuals.

Number of New Hampshire Residents Affected
One NH resident was affected by this incident.

Steps taken in response to the breach
We have no evidence that personal information has been misused. Upon learning of this incident, we took immediate steps to stop the unauthorized access to email accounts and, other than this incident, have no evidence of further unauthorized activity on our systems. We take the protection of personal data seriously and are taking additional security steps, including implementing more measures to strengthen the security of our systems. We have improved our firewall to block intruder attempts, have updated employee passwords to be more complex, and trained our employees on security awareness. Our cyber forensic experts are providing ongoing recommendations on other measures we can implement to prevent a recurrence of a similar incident.

Sample Notice Letter
Enclosed is a copy of the notice being sent to the NH resident on October 24, 2018 which details information about no-cost credit monitoring and other services we are making available for the next 24 months.

Please contact me if you have any questions or need further information.

Sincerely,

Gulshan Shaver

Gulshan Shaver
gshaver@guardanthealth.com
Enclosure: Representative sample notification letter to New Hampshire resident

GUARDANT

Processing Center • P.O. BOX 141578 • Austin, TX 78714

Notice of Data Breach

October 22, 2018

Dear [Name],

We are writing to inform you of an incident that may have resulted in unauthorized access to your personal information.

What Happened

On August 23, 2018, Guardant Health learned that certain company shared email accounts may have been accessed by an unauthorized actor. We promptly took steps to stop the unauthorized access and began an investigation with a leading cyber forensics firm to help us determine what data may have been accessed as a result of this incident. In the course of our investigation, we determined that there may have been access to personal information in the email messages on these accounts during a period of time between February 24 and August 14, 2018. On September 13, 2018, our investigation was able to determine what information may have been breached and what individuals may have been impacted. Based on these results, we believe your information may have been included in this incident.

What Information Was Involved

The personal information impacted may have included your name, home address, social security number, bank account information (if electronic payment was set up), date of birth and other information you may have submitted on a W-9 form.

What We Are Doing To Protect Your Information

We have no evidence that your personal information has been misused. Upon learning of this incident, we took prompt steps to stop the unauthorized access to email accounts and have no evidence of further unauthorized activity on our systems. We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence, including implementing additional measures to strengthen the security of our systems. We have improved our firewall to block potential future intruder attempts, have updated employee passwords to be more complex, and educated our employees to be alert for suspicious email activity. Furthermore, our cyber forensic experts are providing us with ongoing recommendations on additional measures we can implement to prevent a recurrence of a similar incident.

What You Can Do

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-725-5770 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-725-5770 using the following redemption code: [Redemption Code].

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

For More Information

If you have further questions or concerns about this incident, please contact our incident call center at 1-855-725-5770. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Gulshan Shaver
VP, Legal Affairs and Chief Compliance Officer
Guardant Health, Inc.
505 Penobscot Drive, Redwood City, CA, 94063

Information about Identity Theft Protection

We recommend that you 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 below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records.

You may want to review tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website athttp://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

Maryland residents may want to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

North Carolina residents may want to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

Oregon residents are advised to report any suspected identity theft to law enforcement, including the Oregon Attorney General and the Federal Trade Commission. The Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301 or at www.doj.state.or.us. The Oregon Consumer Protection Hotlines may be reached toll-free at (877) 877-9392 or at help@oregonconsumer.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077