BAYLORGENETICS

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Baylor Genetics ("Baylor Genetics"). We are writing with important information regarding a recent data security incident that may have involved some of your information. Baylor Genetics is a laboratory located in Houston, Texas that performs specialized genetic tests. Baylor Genetics receives samples directly from ordering physicians as well as from other laboratories that do not perform the specific genetic test or tests ordered by a patient's physician. You previously had testing performed at the direction of your physician. One or more of those tests were referred by your physician to Baylor Genetics. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Baylor Genetics was the target of an email phishing campaign that resulted in a limited number of employees receiving a suspicious email containing a malicious link. These employees unfortunately fell victim to the phishing campaign, resulting in an unauthorized individual gaining access to those employees' email accounts. Upon learning of the incident, Baylor Genetics disabled the impacted email accounts and required mandatory password resets to prevent further misuse.

There is no evidence that the purpose of the phishing campaign was to obtain patient information and we have no evidence that any of your information was actually acquired or used by the unauthorized individual. However, out of an abundance of caution, we are providing notice and offering you identity monitoring services at no charge.

What We Are Doing.

Upon learning of this issue, we immediately commenced a thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive and time-consuming forensic investigation as well as a comprehensive manual document review, we discovered on July 16, 2020 that one or more of the email accounts that were accessed between September 24, 2019 and November 14, 2019 contained some of your personal and/or protected health information.

Since the date of this incident, we have taken several steps to implement additional technical safeguards on our email system to prevent the recurrence of similar incidents. We have also implemented additional training and education for our employees to increase awareness of the risks of malicious emails, including how employees can identify and handle malicious emails.

What Information Was Involved.

The impacted email account(s) contained some of your protected health information, including your [redacted]. Your Social Security number, test results, and financial information **were not** included in the information that may have been accessed.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we have chosen to make you aware of the incident. To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks, including instructions on how to activate your complimentary one-year membership, please see the additional information provided on the following pages. Additionally, this letter provides precautionary measures you can take to protect your medical information.

For More Information.

Please accept our apologies that this incident occurred. We have taken necessary steps to prevent this from happening again. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it and to prevent subsequent occurrences. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do if you are concerned about potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

[redacted]

Baylor Genetics

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Identity Detection and Resolution Services.

ACTIVATE IDENTITYWORKS NOW IN THREE EASY STEPS

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

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 1-877-890-9332 by [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

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

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists 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.

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 [redacted]. 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 (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 one year 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.

* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.