EXHIBIT 1

By providing this notice, Baylor Genetics does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around June 15, 2026, Baylor Genetics identified suspicious activity within a limited portion of its information technology environment. Baylor Genetics immediately secured affected systems and launched a comprehensive investigation with the assistance of leading independent cybersecurity and digital forensic specialists.

The investigation determined that an unauthorized third party accessed certain portions of the Baylor Genetics network, and certain data stored on the network, between June 11 and June 17, 2026. Baylor Genetics then conducted a detailed and time-intensive review to determine what information may have been involved and which individuals were potentially affected. That review was completed on or about July 30, 2026.

Following completion of this review, Baylor Genetics is providing notice to potentially affected individuals in accordance with applicable legal requirements because the investigation determined that certain information relating to them was within the impacted data.

The information that could have been subject to unauthorized access includes name, medical information, and health insurance information.

Notice to Washington Residents

On August 14, 2026, Baylor Genetics began providing written notice of this incident to approximately twenty-seven thousand two hundred forty-three (27,243) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon identifying the event, Baylor Genetics moved quickly to investigate and respond to the same, assess the security of Baylor Genetics systems, and identify potentially affected individuals. Further, Baylor Genetics notified federal law enforcement regarding the event. Baylor Genetics also enhanced monitoring and security controls, strengthened identity and access management, and implemented additional safeguards to further protect sensitive information.

Baylor Genetics is providing access to credit monitoring services where required for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Baylor Genetics is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national

consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and Explanation of Benefits statements, and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Baylor Genetics is also providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Baylor Genetics is also notifying the U.S. Department of Health and Human Services, and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Baylor Genetics
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: November 14, 2026
To Enroll, Scan the QR Code Below:

SCAN ME

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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

August 14, 2026

NOTICE OF <<SECURITY EVENT / DATA BREACH>>

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

Baylor Genetics is writing to inform you of a recent cybersecurity incident that impacted a limited portion of our information technology environment and potentially involved some of your personal information. We recognize that receiving a letter like this can be concerning, and we want to provide clear information about what happened and the steps we are taking to support you. Protecting the privacy and security of the information entrusted to us is among our highest priorities. Upon identifying the incident, we immediately secured our systems, engaged leading independent cybersecurity and digital forensic specialists, and launched a comprehensive investigation. Although we are not aware of any confirmed identity theft, fraud, or misuse of your personal information related to this incident, we are providing you with information about what occurred, the actions we have taken, and resources available to help protect your information.

What Happened? On or around June 15, 2026, Baylor Genetics identified suspicious activity within a limited portion of its information technology environment. We immediately secured affected systems and launched a comprehensive investigation with the assistance of leading independent cybersecurity and digital forensic specialists.

The investigation determined that an unauthorized third party accessed certain portions of our network, and certain data stored on our network, between June 11 and June 17, 2026. Baylor Genetics then conducted a detailed and time-intensive review to determine what information may have been involved and which individuals were potentially affected. That review was completed on or about July 30, 2026.

Following completion of this review, Baylor Genetics is providing notice to potentially affected individuals in accordance with applicable legal requirements because our investigation determined that certain information relating to you may have been contained within the impacted data.

What Information Was Involved? Based on our review, the information that may have been involved for you includes your name together with one or more of the following: [redacted]

At this time, Baylor Genetics is not aware of any confirmed identity theft, fraud, or misuse of your personal information related to this incident.

What We Are Doing. Protecting the confidentiality, privacy, and security of the information entrusted to Baylor Genetics is one of our highest priorities. Immediately after identifying this incident, we secured affected systems, conducted a comprehensive forensic investigation, engaged leading independent cybersecurity and digital forensic

specialists, coordinated with law enforcement and appropriate regulatory authorities, enhanced monitoring and security controls, strengthened identity and access management, and implemented additional safeguards to further protect sensitive information.

We also completed a comprehensive review to identify potentially affected individuals so that we could provide accurate notice based on the facts of our investigation rather than notify individuals before we understood the full scope of the incident. While we are not aware of any confirmed misuse of personal information related to this incident, we are nonetheless offering complimentary credit monitoring and identity protection services for <<12/24 months>> through IDX at no cost to you. Enrollment information is included with this letter below.

What You Can Do. As a precaution, we encourage you to review your account statements, Explanation of Benefits statements, and credit reports for any unusual activity. We also encourage you to enroll in the complimentary identity protection services being offered and review the enclosed *Steps You Can Take to Protect Personal Information*, which includes additional information about fraud alerts, credit freezes, and other resources available to you.

For More Information. We understand that you may have questions regarding this incident. If you have additional questions, please contact our dedicated assistance line at [redacted]. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time, excluding holidays. You may also write to us at 2450 Holcombe Blvd., Suite 2210 Houston, TX 77021.

We sincerely regret any concern or inconvenience this incident may cause. We understand how important it is to safeguard your personal information and we are committed to continually strengthening our cybersecurity and data protection practices.

Sincerely,

Baylor Genetics

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is November 14, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-866-200-0985 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [redacted] Rhode Island residents that may be impacted by this event.