

 **BIRCH  
MEDICAL**  
329 Howe Street, 2191  
Vancouver, BC V6C3N2

Feb 27, 2025

**Office of the Attorney General**  
**Attn: Security Breach Notification**  
**200 St. Paul Place**  
**Baltimore, MD 21202**  
**Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)**

**Re: Notice of Data Event**

To Whom It May Concern:

Birch Medical, located at 8 The Green, Suite B Dover Delaware 19901, is writing to notify your office of an incident that involves certain information relating to 51 Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission.

**Nature of the Data Event**

In September 2024, Birch Medical became aware that unauthorized individuals may have accessed information stored in a folder within Birch Medical's computer systems. An investigation into the incident followed, but the investigation was unable to confirm whether any files within the folder were accessed by any unauthorized individuals. Since learning of the incident, Birch Medical has implemented additional technical and administrative safeguards to protect information within its care. Although the investigation was unable to confirm any unauthorized access to the folder, out of an abundance of caution, a thorough and detailed review of the folder was completed to determine whether the within files contained sensitive information and to whom that information relates. The review was recently completed, and Birch Medical is notifying individuals whose information was stored in the reviewed folder out of an abundance of caution.

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

**Notice to Maryland Residents**

On or about February 27, 2025 Birch Medical provided written notice of this incident to 51 Maryland residents out of an abundance of caution. Written notice is being provided in substantially the same form as the letter attached hereto.

**Other Steps Taken and To Be Taken**

Upon learning of the incident, Birch Medical worked to investigate and respond to the incident, assess the security of the at-issue folder, and identify potentially affected individuals. Birch Medical is also working to implement additional safeguards and training to its employees. Additionally, although there is no evidence of unauthorized access to individuals' information, Birch Medical is providing individuals whose information was in the folder with guidance on how to better protect against identity theft and fraud, if they deem appropriate. Although Social Security numbers, other government issued identification numbers, and financial information were not involved in this incident, Birch Medical is also providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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 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.

Birch Medical is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the incident, please contact us at 604-423-4050.

Very truly yours,



Alyssaa Delmars  
Clinical Director



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



Name

Address

City, State, ZIP CODE



February 27, 2025

**Re: Notice of Data Breach**

Dear Name:

Birch Medical writes to inform you of an incident that may involve some of your information. Birch Medical provides virtual medical consulting services to patients, and you are receiving this letter because Birch Medical processed your health information or otherwise provided you with medical services relating to a medical scan. This letter provides information about the incident, steps Birch Medical has taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

**What Happened.** In September 2024, Birch Medical became aware that unauthorized individuals may have accessed information stored in a folder within Birch Medical's computer systems. An investigation into the incident followed, but the investigation was unable to confirm whether any files within the folder were accessed by any unauthorized individuals. Since learning of the incident, Birch Medical has implemented additional technical and administrative safeguards to protect information within its care. Although the investigation was unable to confirm any unauthorized access to the folder, out of an abundance of caution, a thorough and detailed review of the folder was completed to determine whether the within files contained sensitive information and to whom that information relates. The review was recently completed, and Birch Medical is notifying individuals whose information was stored in the reviewed folder out of an abundance of caution.

**What Information Was Involved.** Although Social Security numbers, government issued identification numbers, and financial information were not involved in this incident, some of your health information may have been affected, including your medical information, and name.

**What We Are Doing.** Birch Medical prioritizes its responsibility to safeguard the information in its possession. As such, Birch Medical responded upon learning of this incident and has worked diligently to provide you with accurate and complete notice of the incident as soon and accurately as possible. As part of its ongoing commitment to the privacy and security of information in its care, Birch Medical continues to review its existing policies and training protocols relating to data protection on an ongoing basis designed to better prevent similar incidents in the future.

**What You Can Do.** In accordance with best practices, as would be recommended in response to any data incident, Birch Medical encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next 12 to 24 months. Any questionable activity detected should be reported to the associated insurance companies, health care provider, or financial institution promptly and without delay. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*.

**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, you may reach Birch Medical at: 1-877-825-0515 from 6 am – 6 pm Pacific Time Monday through Friday, except holidays. You may also write to us at 8 The Green Ste B, Dover DE, 19901.

Sincerely,

Alyssaa Delmars, Clinical Director



## Steps You Can Take To Protect Personal Information

### 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](http://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 one-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 fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

| <b>Equifax</b>                                                                                                                  | <b>Experian</b>                                                             | <b>TransUnion</b>                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045                                                                                                                  | 1-888-397-3742                                                              | 1-800-916-8800                                                                              |
| Equifax Fraud Alert, P.O. Box 105069<br>Atlanta, GA 30348-5069                                                                  | Experian Fraud Alert, P.O. Box<br>9554, Allen, TX 75013                     | TransUnion Fraud Alert, P.O. Box<br>2000, Chester, PA 19016                                 |
| Equifax Credit Freeze, P.O. Box 105788<br>Atlanta, GA 30348-5788                                                                | Experian Credit Freeze, P.O.<br>Box 9554, Allen, TX 75013                   | TransUnion Credit Freeze, P.O.<br>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](http://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](http://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/>. Birch Medical is located at 8 The Green Ste B, Dover DE, 19901.

*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](http://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](http://www.ncdoj.gov).

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