



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

March 20, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent OrthoMinds, LLC (“OrthoMinds”) located at 12600 Deerfield Parkway, Suite 100, Alpharetta, GA 30004, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twenty-eight (28) Maryland residents. OrthoMinds is providing notice on behalf of the following entities (“Clients”) and the total number of impacted individuals in parenthesis below:

- Comfort Dental Braces - San Antonio, 3023 Thousand Oaks, Suite 108, San Antonio, TX 78247, one (1).
- Lee Orthodontics, 3002 South Clack Street, Abilene, TX 79606, six (6).
- WOW! Smiles, 2180 Northpoint Parkway, Santa Rosa, CA 95407, twenty-one (21).

Notice and the investigation in this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, OrthoMinds does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

In November 2024, OrthoMinds learned of a potential incident within its networked environment. Upon discovery, OrthoMinds launched an investigation into the nature and scope of this potential incident, including remediation efforts. Upon further investigation, OrthoMinds determined that files and folders stored on certain databases may have been accessible to others outside of our

organization between November 17, 2024, and November 27, 2024. As a result, OrthoMinds remediated to prevent the potential for ongoing access and began an extensive review of these files and folders to determine whether sensitive information may be impacted. OrthoMinds then worked with its clients to compile and finalize lists of potentially impacted individuals. OrthoMinds, is notifying on behalf of the covered entities list above.

Although the information varies for each individual, the potentially impacted data includes name, payment card information, medical information, and health insurance information. OrthoMinds coordinated notification with covered entities and is providing notice to individuals and regulators, as directed, on covered entities behalf.

Notice to Maryland Residents

On or about March 20, 2024, OrthoMinds began providing written notice of this incident to twenty-eight (28) Maryland 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 discovering the event, OrthoMinds moved quickly to investigate and respond to the incident, assess the security of OrthoMinds systems, and identify potentially affected individuals.. OrthoMinds is also working to implement additional safeguards. OrthoMinds is providing access to credit monitoring services for twelve (12) months, through IDX, to certain individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, OrthoMinds is providing impacted individuals with guidance on how to better protect against identity theft and fraud. OrthoMinds is 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 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.

OrthoMinds is providing written notice of this incident to relevant state and federal regulators, as necessary.

Office of the Attorney General

March 20, 2025

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/mls
Enclosure

EXHIBIT A



Return Mail Processing Center:

<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 20, 2025

NOTICE OF <<SUBJECT LINE>>

Dear <<Name 1>> <<Name 2>>:

OrthoMinds, LLC ("OrthoMinds"), is writing to inform you of an incident that may impact the security of some of your information. OrthoMinds is a software company that provides orthodontic software services to its clients, including <<Variable Data 2 (data owner name)>>. While we are unaware of any actual or attempted misuse of your information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? In November 2024, OrthoMinds learned of a potential incident within its networked environment. Upon discovery, OrthoMinds launched an investigation into the nature and scope of this potential incident, including remediation efforts. Upon further investigation, OrthoMinds determined that files and folders stored on certain databases may have been accessible to others outside of our organization between November 17, 2024, and November 27, 2024. As a result, OrthoMinds remediated to prevent the potential for ongoing access and began an extensive review of these files and folders to determine whether sensitive information may be impacted. Following the investigation, OrthoMinds reported this incident to its clients, including <<Variable Data 2 (data owner name)>>. OrthoMinds then worked with its clients to compile and finalize lists of potentially impacted individuals.

What Information Was Involved? OrthoMinds is notifying you now because the investigation recently determined that certain information relating to you may have been within the accessed systems. The personal information involved in this incident may have included your name and <<Variable Data 3 (Data Elements Impacted)>>. Please note that we have no evidence to suggest that any information has been misused to date as a result of this incident.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon discovering the unauthorized activity, we took steps to further increase the security of our systems and investigated the activity. As part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to prevent similar future incidents. We are also reviewing and enhancing existing policies and procedures.

As an added precaution, OrthoMinds is offering you complimentary access to <<12/24>> months of credit monitoring through IDX. Details of this offer and instructions on how to enroll in the services may be found in the attached *Steps You Can Take to Help Protect Your Personal Information*. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the offered identity monitoring services.

What You Can Do. We encourage you to remain vigilant against events of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to review the information contained in them enclosed *Steps You Can Take to Help Protect Your Personal Information*.

For More Information. If you have additional questions or need assistance, please call our dedicated assistance line at 1-877-720-2832 Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time. You can also write to OrthoMinds at 12600 Deerfield Parkway, Suite 100, Alpharetta, GA 30004. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

OrthoMinds, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in IDX Credit 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 enrollment deadline is June 20, 2025.

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 1-877-720-2832 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

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all account activity is valid. Report any questionable charges promptly to the company with which the account is maintained.

Order Your Free Credit Report

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. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

Fraud Alerts & Security Freezes

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 place a security freeze on your credit report, you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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 credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	www.transunion.com/credit-freeze https://www.transunion.com/fraud-alerts
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 Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Once you have submitted your request, the credit reporting bureau must place the credit freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than 5 business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

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 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.