



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 1, 2023

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 Oregon Academy of General Dentistry (“OAGD”) located at 13333 SW 68th Parkway, #010, Tigard, OR 97223, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, OAGD 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

On October 31, 2022, OAGD discovered suspicious activity related to an employee’s email account. OAGD promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor accessed the employee email account between October 17, 2022 and October 31, 2022. However, the investigation was unable to determine which, if any, emails and attachments in the account were viewed by the unauthorized person(s). Out of an abundance of caution, OAGD undertook a thorough review of the account’s contents to determine whether any personal information may have been accessible to the unknown actor during the limited period of unauthorized access. This review recently concluded, and OAGD is providing notice to potentially impacted individuals in an abundance of caution.

The personal information that could have been subject to unauthorized access includes name, Social Security number, and payment card information.

Mullen.law

Notice to Maryland Residents

On or about March 1, 2023, OAGD provided written notice of this incident to one (1) Maryland resident. 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, OAGD moved quickly to investigate and respond to the incident, assess the security of OAGD systems, and identify potentially affected individuals. OAGD is also working to implement additional safeguards, including implementing multi-factor authentication, IT auditing review, and providing additional training to its employees. OAGD is providing access to credit monitoring services for 1 year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

OAGD is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/lhw
Enclosure

EXHIBIT A



<<Return Mail Address>>

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

<<Address 1>>

<<Address 2>>

<<Date>>

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

<<Country>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Oregon Academy of General Dentistry (“OAGD”) writes to notify you of a recent event that may affect the privacy of your personal information. Although we have no indication that your information has been misused or that fraud has taken place, we are providing you with details about the event, our response, and steps you can take to protect your personal information, should you feel it appropriate to do so.

What Happened? On October 31, 2022, OAGD discovered suspicious activity related to an employee’s email account. OAGD promptly commenced an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor accessed the employee email account between October 17, 2022 and October 31, 2022. However, the investigation was unable to determine which, if any, emails and attachments in the account were viewed by the unauthorized person(s). Out of an abundance of caution, OAGD undertook a thorough review of the account’s contents to determine whether any personal information may have been accessible to the unknown actor during the limited period of unauthorized access. Based on the results of this review, OAGD is providing you with this notification in an abundance of caution.

What Information Was Involved? Our investigation determined the following information relating to you was present in the email account during the period of unauthorized access: name, <<Data Elements>>. Please note, we have no evidence that your personal information was taken or misused as a result of this event.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. In response to the security incident, we promptly took steps to secure the email account, including by rotating passwords, implementing multi-factor authentication, and conducted a diligent investigation aided by third-party forensic specialists, to confirm the full nature and scope of the event.

As an added precaution, we are also providing you with access to 12 months of complimentary identity monitoring and restoration services through Experian, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will also find more information about the identity monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call [call center toll-free number], Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST, excluding U.S. holidays. You may also write to us at: 13333 SW 68th Parkway, #010, Tigard, OR 97223.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy of information in our possession.

Sincerely,

Lauren Malone

Lauren Malone, CMP
Executive Director
Oregon Academy of General Dentistry

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Protection

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 12 months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B#####] 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:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
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

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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/>.