OREGON ENDODONTIC GROUP
LEILA TARSA D.D.S., M.S.
Practice Limited to Endodontics

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

Oregon Endodontic Group is writing to advise you of a recent event that may impact the security of your personal information. While we are unaware of any actual or attempted misuse of the protected health information, we write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

What Happened? On November 13, 2018, Oregon Endodontic Group discovered suspicious activity in the company's email account. Oregon Endodontic Group immediately began an investigation to determine what happened and what information may have been affected. A third-party forensic investigator was also retained to assist with the investigation. The investigation revealed that malware was downloaded to the company's front office computer on November 9, 2018. This malware has the ability to exfiltrate data from emails. As part of the investigation, Oregon Endodontic Group was unable to rule out data from the office's email account being exfiltrated. The email account was then reviewed to determine whether it contained any protected health information. On February 11, 2019, Oregon Endodontic Group confirmed that the email account contained protected health information of certain current and former patients. Oregon Endodontic Group does not have evidence the information in the email account was exfiltrated. However, the malware impacting the office's computer has such capability and Oregon Endodontic Group cannot rule out exfiltration of the data from emails.

What Information Was Involved? The email accounts subject to unauthorized access contained the following types of information relating to you: your <<ClientDef1(name[and/,][data elements])>><<ClientDef2([data elements])>>.

What We Are Doing. Oregon Endodontic Group is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we stopped using the impacted computer and began using a different computer. We are consulting with a technology firm about adding additional security measures. We are also notifying potentially affected individuals about the incident so that they may take further steps to best protect their personal information, should they feel it is appropriate to do so. We are also notifying any required federal and state regulators.

What You Can Do. You can review the attached Steps You Can Take to Protect Against Identity Theft and Fraud.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-???-???-????, Monday through Friday, 6:00 a.m. to 3:30 p.m. PT (excluding some U.S. holidays). We sincerely regret the inconvenience this incident causes for you. Oregon Endodontic Group remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Leila Tarsa

Dr. Leila Tarsa

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.