NOTICE OF DATA PRIVACY EVENT

Oregon Endodontic Group recently discovered an incident that may affect the security of personal information of certain current and former patients. We take this incident very seriously and the confidentiality, privacy, and security of our information is one of our highest priorities.

What Happened? On November 13, 2018, Oregon Endodontic Group became aware of suspicious activity in the office's email accounts. We 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 a piece of malware known as Emotet was downloaded to the office's computer on November 9, 2018. Emotet 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. The types of information contained within the email account varied by individual but included name and one or more of date of birth, treatment/diagnosis information or health insurance information for most of the affected individuals. In addition, name and Social Security number was included for forty-one (41) individuals, name and driver's license number for two (2) individuals, and name and financial account information for seven (7) individuals. 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 the exfiltration of the data.

Oregon Endodontic Group is not aware of any reported attempted or actual misuse of any protected health information as a result of this event.

What is Oregon Endodontic Group doing in response to this incident? 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 also 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 should I do in response to this incident? Oregon Endodontic Group encourages you to remain vigilant against incidents of identity theft and fraud. You should review your account statements or your loved ones' account statements for suspicious activity. If you see any unauthorized charges, promptly contact the bank or credit card company. We also recommend reviewing your credit report for inquiries from companies that you have not contacted, accounts you did not open and debts on your accounts that you cannot explain.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. Oregon Endodontic Group encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms 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.

Security Freeze 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 2002 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Additional Information

Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission. **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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

If you have questions or concerns that are not addressed in this notice, you may call the dedicated assistance line we've established regarding this incident. Please call 866-297-8759 Monday through Friday, 6:00 a.m. to 3:30 p.m. PT (excluding some U.S. holidays).