MONTGOMERY PURDUE BLANKINSHIP & AUSTIN PLLC

MPBA
Attorneys/Seattle

5500 COLUMBIA CENTER
701 FIFTH AVENUE
SEATTLE, WA 98104-7096
(206) 682-7090 TEL
(206) 625-9534 FAX

LUKE J. CAMPBELL
ATTORNEY AT LAW
lcampbell@mpba.com

October 29, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent MK Periodontics and Implants ("MK Periodontics") located at 2302 S. Union Ave, Building C, Suite 27, Tacoma, WA 98405, and are writing to notify your office of an incident that may affect the security of personal information relating to 8,000 Washington residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission.

Nature of the Data Event

On August 30, 2020, MK Periodontics learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Because the impacted systems contained patient information, MK Periodontics worked quickly to (1) restore access to the patient information so it could continue to care for patients without disruption and (2) investigate what happened and whether this incident resulted in any unauthorized access to, or theft of, patient information by the unknown actor.

MK Periodontics conducted an extensive investigation, with the assistance of third-party computer specialists to determine the nature and scope of the incident. This investigation determined that the particular type of ransomware used in this attack encrypts data but does not usually exfiltrate or remove any data. However, the investigation was unable to confirm no data was actually exfiltrated. The full extent of information that was accessed by the unknown actor is not known. In an abundance of caution, MK Periodontics performed a comprehensive review of all information stored in its systems at the time of incident to identify the individuals whose information may have been accessible to the

unknown actor. MK Periodontics then worked to determine the identities and contact information for potentially impacted individuals.

Although the types of personal information potentially impacted varies by individual, the types of personal information potentially impacted for Washington residents includes: name, address, date of birth, patient identification, social security number (if on file), credit card information (if on file), facility, treating dentist, medical history, procedures performed, and recommendations on future procedures.

Notice to Washington Residents

MK Periodontics is a covered entity under the federal health insurance portability and accountability act of 1996, 42 U.S.C. Sec. 1320d et seq., and provided notice to affect patients in compliance with section 13402 of the federal health information technology for economic and clinical health act, P.L. 111-5 as it existed on July 24, 2015, which notice, pursuant to RCW 19.255.030, also satisfies the requirements of Chapter 19.255 RCW.

Specifically, on October 29th, 2020 MK Periodontics began providing written notice of this incident to affected individuals. Written notice was provided to affected individuals in substantially the same form as the letter attached here as Exhibit A. On October 29th, 2020, MK Periodontics ordered publication of a legal notice of the incident in The Tacoma News Tribune in substantially the same form as attached here as Exhibit B. Additionally on October 29th, 2020, MK Periodontics provided notice to prominent media outlets in Washington in substantially the same form as the notice attached here as Exhibit C. Finally, on October 29th, 2020, MK Periodontics provided notice to the Secretary of Health and Human Services in substantially the same form as the notice attached here as Exhibit D.

Other Steps Taken and To Be Taken

Upon discovering the potential unauthorized access to personal information as a result of the ransomware attack, MK Periodontics moved quickly to identify those that may be affected, put in place resources to assist them, and provide them notice of this incident. MK Periodontics is also working to implement additional safeguards to protect the security of information in its systems.

MK Periodontics is providing written notice to those individuals who may be affected by this incident. This notice includes the contact information for a dedicated assistance line for potentially affected individuals to call with questions or concerns regarding this incident. Additionally, MK Periodontics is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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 report attempted or actual identify theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (206) 682-7090.

Sincerely,

Luke J. Campbell

LJC:bmm
Enclosures
cc: MK Periodontics

EXHIBIT A

MK Periodontics and Implants
2302 S Union Avenue Suite C-27
Tacoma WA, 98405

October 28th, 2020

Patient Name
Address
City, State Zip

Re: Notice of Data Breach

«GreetingLine»

We value and respect the privacy of your information, which is why we are writing to advise you of a recent data security incident that may have involved some of your personal information. On August 29, 2020, MK Periodontics and Implants learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. **We have no reason to believe that your information has been misused to commit fraud or identity theft; however, we are providing guidance on how you can protect yourself.**

Upon learning of the incident, MK Periodontics and Implants promptly removed the "ransomware" software, restored the vast majority of patient information so we could continue to care for patients without disruption, and implemented new policies and procedures to further enhance security. An extensive investigation was conducted, with the assistance of Legal Counsel and third-party computer specialists to determine the nature and scope of the event. **This investigation did not find any evidence that personal information was accessed or exfiltrated by the attacker**, but it also could not definitively rule out this possibility. The information at issue could include your name, patient number, and in some cases, address, contact information, social security number and credit card information (if provided to MK Periodontics and Implants), as well as other personal health information related to treatment by MK Periodontics and Implants.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed Steps You Can Take to Help Protect Your Information. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanations of benefits, and to monitor your credit reports for suspicious activity.

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including reviewing our technical controls. For further information and assistance, please call 1-888-441-0788 from 8am-3pm, Monday through Thursday.

Sincerely,

MK Periodontics and Implants

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

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	**Transunion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com	www.transunion.com	www.equifax.com

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 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com	www.transunion.com	www.equifax.com

Additional 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.

For Washington State residents: The Attorney General can be contacted by mail at Office of the Attorney General, 1125 Washington St SE, P.O. Box 40100 Olympia, WA 98504, (360) 753-6200, 1-800-551-4636, or online at https://www.atg.wa.gov.

EXHIBIT B

MK Periodontics and Implants, **NOTICE OF DATA BREACH INCIDENT**

On August 29, 2020, MK Periodontics and Implants learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Upon learning of the incident, MK Periodontics promptly removed the "ransomware" software, restored the vast majority of patient information, and implemented new policies and procedures to further enhance security. An extensive investigation was conducted, with the assistance of Legal Counsel and third-party computer specialists to determine the nature and scope of the event. **This investigation did not find any evidence that personal information was accessed or exfiltrated by the attacker**, but it also could not definitively rule out this possibility. The information at issue could include your name, patient number, and in some cases, address, contact information, social security number and credit card information, as well as information related to treatment by MK Periodontics. **While we have no reason to believe that your information has been misused to commit fraud or identity theft; we are providing guidance on how you can protect yourself.** MK Periodontics 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 for suspicious activity. Mailed notification letters have been sent to all individuals whose information may have been affected. We are also providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files. The relevant contact information includes: Equifax 1-888-766-0008 www.equifax.com, Experian 1-888-397-3742 www.experian.com, and Transunion 1-800-680-7289 www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, 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. We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-888-441-0788 from 8am-3pm, Monday through Thursday.

EXHIBIT C

Press Release, October 29, 2020

MK Periodontics and Implants, **NOTICE OF DATA BREACH INCIDENT**

On August 29, 2020, MK Periodontics and Implants learned that its electronic medical records system had become encrypted due to "ransomware" deployed by an unknown actor. Upon learning of the incident, MK Periodontics promptly removed the "ransomware" software, restored the vast majority of patient information, and implemented new policies and procedures to further enhance security. An extensive investigation was conducted, with the assistance of Legal Counsel and third-party computer specialists to determine the nature and scope of the event. **This investigation did not find any evidence that personal information was accessed or exfiltrated by the attacker**, but it also could not definitively rule out this possibility. The information at issue could include your name, patient number, and in some cases, address, contact information, social security number and credit card information, as well as information related to treatment by MK Periodontics. **While we have no reason to believe that your information has been misused to commit fraud or identity theft; we are providing guidance on how you can protect yourself.** MK Periodontics 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 for suspicious activity. Mailed notification letters have been sent to all individuals whose information may have been affected. We are also providing potentially impacted individuals with contact information for the three major credit reporting agencies, as well as providing advice on how to obtain free credit reports and how to place fraud alerts and security freezes on their credit files. The relevant contact information includes: Equifax 1-888-766-0008 www.equifax.com, Experian 1-888-397-3742 www.experian.com, and Transunion 1-800-680-7289 www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, 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. We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 1-888-441-0788 from 8am-3pm, Monday through Thursday.

EXHIBIT D

Breach Tracking Number: **FS6BFFXHKK**

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification. Your breach notification will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the breach notification you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your breach notification for investigation.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have any additional information to add to your breach notification, you may call 1-800-368-1019. Please reference the number given by OCR when submitting your breach notification.

* Breach Affecting: 500 or More Individuals
* Report Type: Initial Breach Report

* Are you a Covered Entity filing on behalf of your organization? Yes

---

Covered Entity

* Name of Covered Entity: MK Periodontics and Implants
* Type of Covered Entity: Healthcare Provider
* Street Address Line 1: 2302 S Union Avenue
Street Address Line 2: Suite C-27
* City: Tacoma
* State: Washington
* ZIP: 98405

Covered Entity Point of Contact Information

* First Name: Luke * Last Name: Campbell
* Email: lcampbell@mpba.com
* Phone Number: (Include area code): Contact Phones

Phone Number	Usage
(206) 695-1107	Work

* Breach Start Date: 08/14/2020 * Breach End Date: 09/05/2020
* Discovery Start Date: 08/30/2020 * Discovery End Date: 08/30/2020
* Approximate Number of Individuals Affected by the Breach: 8000

---

* Type of Breach: Hacking/IT Incident

---

* Location of Breach: Desktop Computer
Network Server

---

* Type of Protected Health **Clinical**

Information Involved in Breach:	**Demographic** **Financial** * Clinical Diagnosis/Conditions Lab Results Medications Other Treatment Information * Demographic Address/ZIP Date of Birth Drivers License Name SSN Other Identifier * Financial Claims Information Credit Card/Bank Acct # Other Financial Information

---

* Brief Description of the Breach:	On August 29, 2020 one of the employees could not access the Open Dental software through the work network and alerted the IT manager. The next day the IT manager remotely accessed the server (August 30, 2020) and determined ransomware had encrypted the server and all of the files on the server. After numerous attempts to decrypt the data, including communicating with the ransomware attackers, on September 5, 2020 MK Periodontics started over by installing brand new servers, new software, and attempting to recreate all of its patient data. A new firewall, router, hard drives, and upgrades to windows programs were installed on all servers and workstations. A brand new Open Dental database was created, and data that the Open Dental company had saved on their systems from late August 2020 was able to be migrated onto the new database. Most of the patient data was restored for use with the exception of x-ray images and customer attachment files saved as images. The actions taken to restore the data and install new servers and software took place from September 5-7, 2020. Additionally, the Open Dental image folders for patients with last name Pas-Z were recovered and restored to the Open Dental Database on October 26th, 2020. On September 8, 2020 MK Periodontics was able to resume normal operations.

---

* Safeguards in Place Prior to Breach:	Privacy Rule Safeguards (Training, Policies and Procedures, etc.)		
* Individual Notice Provided Start Date:	10/29/2020	Individual Notice Provided Projected/Expected End Date:	10/29/2020
Was Substitute Notice Required?	Yes		
	10 or more		

Was Media Notice Required?	Yes
* Select State(s) and/or Territories in which media notice was provided:	Washington

---

* Actions Taken in Response to Breach:	Adopted encryption technologies Changed password/strengthened password requirements Implemented new technical safeguards Took steps to mitigate harm Other
* Describe Other Actions Taken:	• Engaged Legal Counsel • Informed Malpractice Insurance • Engaged DataWorks Consulting on September 9th, 2020 to perform full network scan and assessment to assess risk and look for any malware, evidence of ransomware attacks remaining files, and make recommendations for improvements. Their reports indicate a low risk to the networks, and further confirmed on October 6, 2020 that their security tools had found no evidence of the Eking ransomware (or any other persistent infection) on the MK Periodontics server. • Hired a consultant, Harris Biomedical, on October 18th, 2020 to help perform a new risk analysis, create a new risk management plan, and create comprehensive policies and procedures for the administrative, physical and technical safeguards. • Hired a new IT company, Uptime Solutions to take over management of MK Periodontics and Implants IT systems. Uptime Solutions, has done their own network assessment and updates and upgrades have begun, including but not limited to the installment of a new firewall system, the adoption of encryption technologies and the approval of a bid to replace the existing in office computer network system to further enhance safety and security. Additionally, Uptime Solutions was able to recover the Open Dental image folders for patients with last name Pas through Z and restored these files to the Open Dental Database on October 26th, 2020. Recovery efforts are ongoing and attempts are being made at recovering the remainder of patient files and x rays.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Veronica Malo Date: *10/29/2020*