Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

February 23, 2023

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Dental Health Management Solutions, located at 2001 Windy Terrace, Suite F, Cedar Park, TX 78613 ("DHMS") with respect to a data security incident described in more detail below. DHMS takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Description of the Incident.

On or about August 20, 2021, DHMS became aware of a possible incident involving its network, which may have resulted in the inadvertent exposure of personal information of individuals, including current and former DHMS patients and employees, to an unknown individual who was not authorized to view it (the "Incident"). DHMS has since worked diligently to determine what happened and what information was involved as a result of this Incident.

Based on the results of an investigation conducted by third-party data mining vendors, DHMS determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, addresses, medical information, health insurance information, Medicaid identification numbers, drivers' licenses, account and routing numbers, and Social Security numbers. The exact elements of personal information that may have been exposed as a result of this incident varies per individual.

As of this writing, DHMS has not received any reports of fraud or identity theft related to this matter.

2. Number of Maine residents affected.

DHMS discovered that the Incident may have resulted in the unauthorized exposure of information pertaining to one (1) Maine resident. A notification letter to this individual was mailed on February 17, 2023, via First Class Mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

3. Steps taken.

DHMS takes the privacy and security of the information within its possession seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Upon discovery of the Incident, DHMS worked with cybersecurity counsel and cyber forensic professionals to investigate how the Incident occurred and what information was compromised. DHMS is committed to ensuring the security of all information within its control, and has taken steps to prevent a similar event from occurring in the future, including the changing of all passwords within its environment and implementation of multifactor authentication. Additionally, the notified Maine resident was offered complimentary identity theft and credit monitoring services for twelve (12) months.

4. Contact information.

DHMS remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN AND DICKER LLP

Anjali C. Das

EXHIBIT A

Dental & Health Management Solutions
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-01762 1-1

Via First-Class Mail

[redacted]

To Enroll, Please Visit:
https://secure.identityforce.com/benefit/dentalhealth

Membership Number:
[redacted]

February 17, 2023

Notice of Data Incident

Dear [redacted]

Dental Health Management Solutions ("DHMS") is writing to inform you of a recent data security incident ("Incident") which may have resulted in unauthorized access to your personal information. DHMS takes the protection and privacy of your information seriously, and we sincerely apologize for any inconvenience this Incident may cause. This letter contains additional information about the Incident, our response to mitigate the Incident, and services available to protect your information.

What Happened

On or about August 20, 2021, DHMS was made aware of a possible incident involving its network. On that same date, DHMS engaged cyber counsel and a specialized third-party cybersecurity firm to assist with securing the environment and to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. On or around October 21, 2021, after a thorough investigation, DHMS found evidence that an unauthorized user had accessed a limited amount of data within its email environment beginning on or about August 5, 2021. Since that time DHMS reviewed the email accounts within its environment to determine whether any of the compromised accounts may have contained sensitive information.

On September 21, 2022, DHMS engaged a specialized third-party data mining firm to conduct a thorough review of one (1) compromised email account that may have contained sensitive information at the time of the Incident. On November 28, 2022, the data mining investigation was completed. Since that time DHMS has aggregated a list of individuals whose information may have been impacted by the incident in order to advise those individuals of its findings with respect to the sensitive information within its possession.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to your: Social Security Number. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the necessary actions in responding to the incident. Together, we continue to closely monitor the situation. DHMS has also notified the FBI and local police departments as to the incident. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future.

As an additional safeguard, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/dentalhealth and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. Enrollment for credit monitoring services requires an internet connection and e-mail account and might not be available for individuals under the age of eighteen (18). Enrolling in this service will not affect your credit score.

You can also obtain more information from the Federal Trade Commission ("FTC") about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident. If you have any questions, please do not hesitate to call 1- 833-570-2898, Monday – Friday, 8:00 am to 8:00 pm Eastern Time.

Sincerely,

Dental Health Management Solutions
2001 Windy Terrace, Suite F
Cedar Park, TX 78613

Additional Important Information

For residents of *Hawaii*, *Michigan*, *Missouri*, *Virginia*, *Vermont*, and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft**For residents of *Massachusetts*:** It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under

the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-report-services/credit-

More information can also be obtained by contacting the Federal Trade Commission listed above.

Free Credit Report Information: Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.
If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".