GT GreenbergTraurig

February 28, 2024

VIA EMAIL

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Knudsen:

We are writing to inform you that our client, Aspen Dental Management, Inc. ("ADMI"), on behalf itself and certain Aspen Dental branded dental practices, is notifying 950 individuals who reside in New Hampshire of a data security incident that impacted some of their personal information.

On April 25, 2023, ADMI was impacted by a ransomware attack. ADMI, with the assistance of leading third-party external security experts, immediately investigated to determine the scope of the incident and restore operations. Following a thorough investigation, including a manual review of hundreds of thousands of documents, we determined personal information belonging to some Aspen Dental patients was subject to unauthorized access. ADMI finished its investigation on February 11, 2023.

The information accessed varied by individual but includes

. ADMI has received assurance that the unauthorized third party no longer has access to any personal information in connection with this incident. ADMI has no indication that any personal information has been misused as a result of the incident.

ADMI takes the security of personal information very seriously and has taken steps to prevent a reoccurrence by increasing the monitoring of its networks, further improving access controls, and hardening its systems. ADMI has notified and is cooperating with federal law enforcement authorities.

ADMI mailed the attached notification to all potentially affected individuals beginning February 22, 2024. The three major Credit Reporting Agencies are also being notified.

ADMI is offering identity theft protection services to individuals who had their Social Security number impacted by this incident through a data breach and recovery service, CyberScout by TransUnion. Services include of credit monitoring, a $1,000,000 identity fraud loss reimbursement, fraud consultation, and identity theft restoration. Information regarding these services, as well as additional information to assist with enrollment, is included in the notification letter mailed to potentially affected individuals.

Please contact me for any additional information.

Best Regards,

Jena Valdetero
Shareholder

JMV:

Enc: Individual Notification Letters

<Return Name>
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

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

February 22, 2024

Dear <<First Name>> <<Last Name>>,

On behalf of your Aspen Dental provider, we are writing to inform you of a data security incident that may have impacted some of your personal information. Aspen Dental takes the security of your personal information very seriously, and we sincerely regret that this occurred. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
On April 25, 2023, Aspen was impacted by a ransomware attack. With the assistance of external cybersecurity experts, we immediately investigated to determine the scope of the incident and to restore operations of our systems. After an extensive review of the files removed from our network, we became aware on December 11, 2023 that your personal information may have been subject to unauthorized access.

What Information Was Involved?
This information included your name along with the following: <<Exposed Data Elements>> We have obtained assurance that the unauthorized third party no longer possesses Aspen documents, and while your personal information was exposed, we have no evidence it has been misused.

What We Are Doing
We take the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by increasing monitoring of our networks, further improving access controls, and hardening our systems.

Out of an abundance of caution, 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 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. We are also 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. With this protection, Cyberscout, a TransUnion company, will help you if you have any identity questions or issues.

What You Can Do
To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/aspendental** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<Unique Code>>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18. When signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We also recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information.

For More Information
Representatives are available for 90 days from the date of this letter to assist you with questions about this incident between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at and supply the fraud specialist with your unique code listed above.

Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Hyung Bak
Chief Legal and Compliance Officer

ADDITIONAL INFORMATION

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 278 Rhode Island residents notified in this incident.

DC Attorney General
400 6th Street NW
Washington, DC 20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain or file a police report.

For residents of all states:

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 www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to 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), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. 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 for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft.

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 by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

<Return Name>
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

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

February 22, 2024

Dear <<First Name>> <<Last Name>>,

On behalf of your Aspen Dental provider, we are writing to inform you of a data security incident that may have impacted some of your personal information. Aspen Dental takes the security of your personal information very seriously, and we sincerely regret that this occurred. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
On April 25, 2023, Aspen was impacted by a ransomware attack. With the assistance of external cybersecurity experts, we immediately investigated to determine the scope of the incident and to restore operations of our systems. After an extensive review of the files removed from our network, we became aware on December 11, 2023 that your personal information may have been subject to unauthorized access.

What Information Was Involved?
This information included your name along with the following: <<Exposed Data Elements>> We have obtained assurance that the unauthorized third party no longer possesses Aspen documents, and while your personal information was exposed, we have no evidence it has been misused.

What We Are Doing
We take the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by increasing monitoring of our networks, further improving access controls, and hardening our systems.

What You Can Do
We recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information.

For More Information
Representatives are available for 90 days from the date of this letter to assist you with questions about this incident between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-919-3310.

Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Hyung Bak
Chief Legal and Compliance Officer

ADDITIONAL INFORMATION

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. There were 278 Rhode Island residents notified in this incident.

DC Attorney General
400 6th Street NW
Washington, DC 20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

New York Attorney General
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

Rhode Island Attorney General
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

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

***Massachusetts and Rhode Island residents*:** You have the right to obtain or file a police report.

For residents of all states:

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 www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to 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), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. 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 for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft.

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 by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800