



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 15, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent the American Dental Association (“ADA”) located at 211 East Chicago Avenue, Chicago, Illinois 60611-2678., and are writing to notify your office of an incident that may affect the security of certain personal information relating to ten (10) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the ADA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 21, 2022, the ADA experienced a disruption to certain computer systems following a sophisticated cyber-attack involving ransomware. The ADA immediately launched an investigation, working with outside cybersecurity specialists to ensure the security of its systems and confirm the nature and scope of this event. On or about April 27, 2022, the ADA determined that certain information stored within its environment may have been accessed and/or acquired by an unauthorized actor. The ADA continued its investigation to confirm what information was stored on impacted systems at the time of the incident, and to whom that information relates. This process involved working with a third-party data mining team to conduct a thorough and time-consuming review of the impacted data. The initial data mining work was completed on or about June 10, 2022. Thereafter, ADA worked diligently to validate the data mining findings, locate address information for potentially affected individuals, and completed that effort on or about July 7, 2022.

The personal information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maryland Residents

On or about July 15, 2022, the ADA provided written notice of this incident to ten (10) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, the ADA moved quickly to investigate and respond to the incident, assess the security of ADA systems, and identify potentially affected individuals. Further, the ADA notified Federal law enforcement regarding the event. The ADA is also working to implement additional safeguards and training to its employees. The ADA is providing access to credit monitoring services for twelve (12) months through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, the ADA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. The ADA is providing individuals with 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 contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The ADA is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/mah
Enclosure

EXHIBIT A



<<Return Mail Address>>

<<Name 1>> <<Name 2>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

<<Country>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Name 1>> <<Name 2>>:

The American Dental Association (“ADA”) writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On or about April 21, 2022, ADA experienced a disruption to certain computer systems following a sophisticated cyber-attack involving ransomware. We immediately launched an investigation, working with outside cybersecurity specialists to ensure the security of our system moving forward and confirm the nature and scope of this event. On or about April 27, 2022, we determined that certain information on ADA’s systems was accessed and/or acquired by an unauthorized actor. We continued our investigation to understand the nature and scope of what occurred, what information was stored on impacted systems at the time of the incident, and to whom that information relates. This process completed on June 10, 2022. ADA worked diligently to locate address information for the potentially affected individuals and just recently completed that effort.

What Information Was Involved? At this time, there is no evidence that any of your personal information has been misused. However, the investigation determined that your name and the following types of personal information related to you were present in the files and folders accessed and/or acquired by the unauthorized actor at the time of the incident: [data elements].

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond, to assess the security of relevant systems, and to reset relevant account passwords. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. ADA notified law enforcement of this incident and will notify relevant state and federal regulators, as appropriate.

We are also offering you access to complimentary credit monitoring and identity protection services for 12 months through Experian. These services include fraud consultation and identity theft restoration services. If you wish

to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. As mentioned previously, there is no evidence to date that any of your personal information has been misused. However, we encourage you to remain vigilant against incidents of identity theft and fraud, and to review your account statements and credit reports for suspicious activity. Additionally, we recommend following best practices when viewing any suspicious emails, including carefully reviewing the email address and domain from the sender, and to refrain from clicking any links provided in unsolicited emails. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you. While ADA will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact [phone number and hours].

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Raymond Cohlma, DDS
Executive Director
The American Dental Association

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration

[Credit/Identity Monitoring Instructions]

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. The American Dental Association is located at: 211 East Chicago Avenue, Chicago, Illinois 60611-2678.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.