



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

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

July 11, 2023

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

To Whom It May Concern:

We represent American Public Health Association (“APHA”) located at 800 I Street NW, Washington, DC 20001, and write to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. The notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, APHA 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 10, 2023, APHA became aware of suspicious activity related to certain APHA computer systems. APHA immediately worked to restore its systems and launched an investigation, with assistance from third-party cybersecurity specialists, to determine the nature and scope of the incident. Through the investigation, it was determined that there was unauthorized access to APHA’s network between April 5, 2023, and April 6, 2023. The investigation determined that the unauthorized actor had access to certain files and folders within its system.

In an abundance of caution, APHA undertook a review of the potentially accessed files to determine the type of information contained within the files and to whom the information related. On June 6, 2023, review of the impacted data was completed, and it was determined that information related to certain individuals was present in the impacted files. APHA then conducted additional review of its files for contact information to notify potentially impacted individuals about the incident.

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

Notice to Maryland Resident

On or about July 10, 2023, APHA provided written notice of this incident to one (1) Maryland resident. 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, APHA moved quickly to investigate and respond to the incident, assess the security of APHA systems, and identify potentially affected individuals. Further, APHA notified federal law enforcement regarding the event. APHA is also working to review its existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on its systems. APHA is providing access to credit monitoring services for twelve (12) months through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

APHA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. APHA 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. APHA notified other state regulators as necessary. Also, APHA notified federal law enforcement and is cooperating with its investigation.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Richard Aponte-Boyd", with a stylized flourish at the end.

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/kzm
Enclosure

EXHIBIT A



To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: [XXXXXXXXXX]

800 I Street, NW
Washington, DC 20001<<Return Mail Address>>

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

<<Address 1>>

<<Address 2>>

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

<<Country>>

<<Date>>

NOTICE OF [SECURITY INCIDENT] / [DATA BREACH]

Dear <<Full Name>>:

American Public Health Association (“APHA”) writes to inform you of a recent event that may involve some of your information. Although there is no indication that your information has been misused in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On or about April 10, 2023, APHA became aware of suspicious activity related to certain APHA computer systems. We immediately worked to restore our systems and launched an investigation, with assistance from third-party cybersecurity specialists, to determine the nature and scope of the incident. Through the investigation, it was determined that there was unauthorized access to APHA’s network between April 5, 2023, and April 6, 2023. The investigation determined that the unauthorized actor had access to certain files and folders within our system.

We undertook a review of the potentially accessed files to determine the type of information contained within the files and to whom the information related. On June 6, 2023, we completed the review of the impacted data and then conducted additional review of our files for contact information to notify potentially impacted individuals about the incident. We are notifying you because some personal information of yours was within the impacted files.

What Information Was Involved? The investigation determined that your name and [Extra2-Data Elements] were included within files that may have been accessed and/or acquired by an unauthorized individual.

What We Are Doing. We at APHA take this event and the security of your information seriously. Upon learning of this event, we moved quickly to investigate and respond to the incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems.

Although we are unaware of any fraudulent misuse of personal information relating to this event, as an added precaution, we are offering you access to [Extra3 – 12/24 months] months of complimentary credit monitoring and identity protection services through IDX at no cost to you. If you wish to activate the credit monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information. You can also enroll to receive the complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company. IDX identity protection services include: [Extra3 – 12/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance

reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

Although we are making these services available to you, we are unable to enroll you directly.

There are two ways you can enroll:

Enrollment URL*: <https://app.idx.us/account-creation/protect>

Enrollment TFN*: 1-800-939-4170

IDX Identity will include [Extra3 - one-year/two-year] enrollments into the following service components:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN TEAM - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

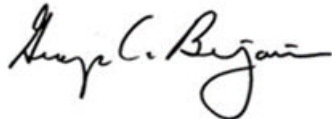
FULLY MANAGED IDENTITY RECOVERY - ID Experts' fully managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

*Your enrollment code expires for use on **02.01.24** but will include a full twelve (12) month service term upon enrollment. However, we'd encourage a 30-60-day enrollment window.

For More Information. We understand that you have my questions about this incident that are not addressed in this letter. If you have additional questions, please call me at 202-777-2430, or contact me via email at georges.benjamin@apha.org. You can also write to APHA at 800 I Street NW, Washington, DC 20001.

We take the privacy and security of personal information in our care very seriously and regret any inconvenience or concern this incident may have caused.

Sincerely,



Georges C. Benjamin, MD
Executive Director
American Public Health Association

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information

listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 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 <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

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.