



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

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

February 26, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Public Health Management Corporation (“PHMC”) located at Centre Square East, 1500 Market Street, Suite 1500, Philadelphia, Pennsylvania, 19102, and are writing to notify your office of an incident that may affect the security of certain personal information relating to nine (9) New Hampshire 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, PHMC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 8, 2023, PHMC became aware of suspicious activity related to certain computer systems. Upon discovery, PHMC immediately launched an investigation, with the assistance of third-party forensic specialists, to secure its network and determine the nature and scope of the activity. The investigation determined that there was unauthorized access to PHMC’s network on May 8, 2023, and the unauthorized actor had the ability to acquire certain information stored on the network during the period of access. PHMC subsequently conducted a comprehensive review of the data determined to be at risk to assess what sensitive information was contained therein and to whom the information relates. On December 20, 2023, PHMC completed this initial review and determined that information related to certain individuals could be impacted. The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On February 26, 2024, PHMC provided written notice of this incident to nine (9) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. In an effort to notify affected individuals as soon as possible, PHMC posted a notice of the event on the homepage of its website and notified the media regarding the event on July 6, 2023.

Other Steps Taken and To Be Taken

Upon discovering the event, PHMC moved quickly to respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, PHMC notified federal law enforcement regarding the event. PHMC is providing individuals whose Social Security number was potentially affected by this incident access to credit monitoring services for , through IDX, at no cost to the individuals.

Additionally, PHMC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. PHMC 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.

PHMC is providing written notice of this incident to relevant state and federal regulators, 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 .

Very truly yours,

Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/kzm
Enclosure

EXHIBIT A



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

February 26, 2024

NOTICE OF DATA EVENT

Dear <<First Name>> <<Last Name>>:

Public Health Management Corporation (“PHMC”) writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On May 8, 2023, PHMC became aware of suspicious activity related to certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to secure our network and determine the nature and scope of the activity. The investigation determined that there was unauthorized access to our network on May 8, 2023, and the unauthorized actor had the ability to acquire certain information stored on the network during the period of access. Therefore, we conducted a comprehensive review of the data determined to be at risk to assess what sensitive information was contained therein and to whom the information relates. On December 20, 2023, we completed this review and determined that information related to certain individuals could be impacted.

What Information Was Involved? We determined the type of information potentially impacted by this incident includes your: <<Data Elements>> .

What We Are Doing. We take the confidentiality, privacy, and security of information in our care seriously. Upon discovering this incident, we immediately commenced an investigation and took steps to implement additional safeguards related to data privacy and security. In an effort to notify affected individuals as soon as possible, we posted a notice of the event on the homepage of our website and notified the media regarding the event on July 6, 2023.

Out of an abundance of caution, we are providing you with access to <<# of Months>> months of credit monitoring and identity protection services through IDX at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through IDX. We also 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.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, or need assistance, please call our dedicated assistance line at 1-888-829-4216, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also write to us at Centre Square East, 1500 Market St., Suite 1500, Philadelphia, PA 19102.

Sincerely,

Public Health Management Corporation

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/phmc> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is May 26, 2024.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-829-4216 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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; 1-410-576-6300 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 12 Rhode Island residents that may be impacted by this event.