



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 03 2021

CONSUMER PROTECTION

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

April 12, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Cuyahoga Metropolitan Housing Authority ("CMHA") located at 8120 Kinsman Road, Cleveland, Ohio, 44104, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. 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, CMHA 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 February 10, 2021, CMHA became aware of suspicious activity within its computer network. CMHA immediately began an investigation to determine the nature and scope of the activity. Our investigation determined that certain files within our environment were encrypted and inaccessible as part of a ransomware attack. On February 26, 2021, we confirmed that certain files had been accessible to unknown actors. CMHA then worked to identify those individuals whose information may have been accessible to the unauthorized actor. To date, we have been unable to determine which specific files were accessed. The information that could have been subject to unauthorized access includes name, address, Social Security number, financial information, or driver's license/state ID number.

Notice to New Hampshire Resident

On or about April 12, 2021, CMHA provided electronic substitute notice of this incident to identified individuals, which includes one (1) New Hampshire resident. Electronic notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. CMHA also provided substitute notice on its website and to PR Newswire.

Other Steps Taken and To Be Taken

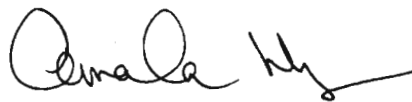
Upon discovering the event, CMHA moved quickly to investigate and respond to the incident, assess the security of CMHA systems, and notify potentially affected individuals. CMHA is also working to implement additional safeguards and training to its employees.

Additionally, CMHA 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. CMHA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,

A handwritten signature in black ink, appearing to read "Amanda Harvey". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Amanda Harvey of
MULLEN COUGHLIN LLC

ANH/eyl

EXHIBIT A

April 12, 2021

RE: Notice of Security Incident

Dear CMHA Stakeholder,

Cuyahoga Metropolitan Housing Authority (“CMHA”) is writing to inform you of recent incident that may affect security of your personal information. While we are unaware of any actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and steps you may take to better protect your personal information, should you feel it necessary to do so.

What Happened? On February 10, 2021, CMHA became aware of suspicious activity within its computer network. CMHA immediately began an investigation to determine the nature and scope of the activity. Our investigation determined that certain files within our environment were encrypted and inaccessible as part of a ransomware attack. On February 26, 2021, we confirmed that certain files had been accessible to unknown actors. CMHA then worked to identify those individuals whose information may have been accessible to the unauthorized actor. To date, we have been unable to determine which specific files were accessed.

What Information was Involved? We have no evidence that your information was subject to actual or attempted misuse. Out of an abundance of caution, CMHA is notifying you of this incident because your name, address, Social Security number, driver’s license number, and/or financial information may have been present in potentially accessed servers. While we cannot confirm if any of your information was accessed, we are informing you of the full scope of what could have been compromised.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities, and we take this incident very seriously. When we discovered this incident, we immediately launched an investigation and took steps to secure our systems and determine what data may be at risk. We are required to notify consumer reporting agencies of this incident, as well. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures and implement additional safeguards.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information.



COMMITMENT ACCOUNTABILITY RESPECT EXCELLENCE SAFETY

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 call CMHA at our dedicated assistance line at 1-855-654-0918, Monday through Friday, 9:00 a.m. to 9:00 p.m. EST, excluding national holidays.

Sincerely,



Jeffery K. Patterson
CMHA Chief Executive Officer



COMMITMENT ACCOUNTABILITY RESPECT EXCELLENCE SAFETY

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.



COMMITMENT ACCOUNTABILITY RESPECT EXCELLENCE SAFETY

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. This notice has not been delayed by law enforcement.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov. Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer. Telephone: 1-888-743-0023. **New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review



COMMITMENT ACCOUNTABILITY RESPECT EXCELLENCE SAFETY

your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfbp_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. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are ten (10) Rhode Island residents impacted by this incident. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



COMMITMENT ACCOUNTABILITY RESPECT EXCELLENCE SAFETY