

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

January 16, 2024

VIA EMAIL (idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Newport News Redevelopment and Housing Authority – Incident Notification

Dear Attorney General Brown:

McDonald Hopkins PLC represents Newport News Redevelopment and Housing Authority, located at 227 27th Street, Newport News, VA 23607. I am writing to provide notification of an incident at Newport News Redevelopment and Housing Authority that may affect the security of personal information of approximately one (1) Maryland resident. Newport News Redevelopment and Housing Authority's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Newport News Redevelopment and Housing Authority does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about June 5, 2023, Newport News Redevelopment and Housing Authority became aware of potentially unauthorized access to their network due to a ransomware cybersecurity incident. Upon learning of this issue, Newport News Redevelopment and Housing Authority immediately contained the threat by disabling all unauthorized access to the network and commenced a prompt and thorough investigation. As part of the investigation, Newport News Redevelopment and Housing Authority has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The forensic investigatory team did not observe the unauthorized party remove any sensitive data from the environment. However, their ability to determine if any data was accessed or taken was limited due to actions taken by the unauthorized actor. Regardless, out of an abundance of caution, Newport News Redevelopment and Housing Authority conducted a thorough and extensive manual review of the data potentially contained on the impacted servers. After several months of extensive efforts to identify, review, and analyze the potentially impacted data, on December 21, 2023, Newport News Redevelopment and Housing Authority determined that the impacted files contained identifiable personal information pertaining to a limited number of individuals. The information that may have been accessed may include full name, Social Security number, and taxpayer identification or IRS PIN. On January 5, 2024, Newport News Redevelopment and Housing Authority located the most

recent address of the impacted individuals. Newport News Redevelopment and Housing Authority proceeded to promptly notify all potentially impacted individuals effectuated on or about January 16, 2024.

As stated above, upon learning of this issue, Newport News Redevelopment and Housing Authority immediately commenced an internal investigation and promptly notified the potentially affected individual. Newport News Redevelopment and Housing Authority has no indication that the information has been used to commit financial fraud or identity theft. Newport News Redevelopment and Housing Authority wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Newport News Redevelopment and Housing Authority is offering the resident with a complimentary membership with a credit monitoring service. Newport News Redevelopment and Housing Authority will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Newport News Redevelopment and Housing Authority will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. A sample of the notice letter is included herein for your reference.

At Newport News Redevelopment and Housing Authority, protecting the privacy of personal information is a top priority. Newport News Redevelopment and Housing Authority is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In response to this incident, Newport News Redevelopment and Housing Authority strengthened data protection measures by taking the following actions: segregated networks and reconfigured access permissions; incorporated 24/7 security monitoring of all PCs, laptops, mobile devices, tablets, and servers using and endpoint detection and response solution; revised technical and administrative policies and procedures; revised backup data procedures; implemented additional employee training via KnowBe4 security awareness training campaigns and email phishing testing; and increased password credential complexity requirements.

Newport News Redevelopment and Housing Authority continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains. If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.



January 16, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Newport News Redevelopment and Housing Authority. We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. Please read this notice carefully as it provides information about the incident and the significant measures we take to protect your information.

What Happened?

On or about June 5, 2023, Newport News Redevelopment and Housing Authority detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of the data we maintain.

What We Are Doing.

Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. We also reported the incident to law enforcement and promptly launched an investigation assisted by external cybersecurity professionals experienced in handling these types of incidents. Our forensic investigatory team did not observe the unauthorized party remove any sensitive data from our environment. However, their ability to determine if any data was accessed or taken was limited due to actions taken by the unauthorized actor. Regardless, out of an abundance of caution, we conducted a thorough and extensive manual review of the data potentially contained on the impacted servers. After several months of extensive efforts to identify, review, and analyze the potentially impacted data, on December 21, 2023, we determined that the impacted files contained identifiable personal information pertaining to a limited number of individuals.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?

The information that may have been accessed contained some of your personal information, including your [REDACTED]

What You Can Do.

We have no evidence that any of your information has been used to commit financial fraud or identity theft as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter also provides other precautionary measures you can take to protect your personal

information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

If you have questions, please contact our dedicated and confidential call center at [REDACTED].

The response line is available for 90 days from the date of this letter, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Newport News Redevelopment and Housing Authority
227 27th Street | P.O. Box 797
Newport News, VA 23607

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

January 16, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

The privacy and security of the personal information we maintain is of the utmost importance to Newport News Redevelopment and Housing Authority. We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and the significant measures we take to protect your information.

What Happened?

On or about June 5, 2023, Newport News Redevelopment and Housing Authority detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the exposure of the data we maintain.

What We Are Doing.

Upon learning of the incident, we immediately took steps to secure our network and mitigate against any additional harm. We also reported the incident to law enforcement and promptly launched an investigation assisted by external cybersecurity professionals experienced in handling these types of incidents. Our forensic investigatory team did not observe the unauthorized party remove any sensitive data from our environment. However, their ability to determine if any data was accessed or taken was limited due to actions taken by the unauthorized actor. Regardless, out of an abundance of caution, we conducted a thorough and extensive manual review of the data potentially contained on the impacted servers. After several months of extensive efforts to identify, review, and analyze the potentially impacted data, on December 21, 2023, we determined that the impacted files contained identifiable personal information pertaining to a limited number of individuals.

While cybersecurity threats continue to impact all of us, we are taking ever-increasing measures to protect the information entrusted to us. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. In response to this incident and through our continuing comprehensive review, we have strengthened our network and implemented additional security improvements recommended by third-party cyber security experts.

What Information Was Involved?

The information that may have been accessed contained some of your personal information, including your [REDACTED]

What You Can Do.

We have no evidence that any of your information has been used to commit financial fraud or identity theft as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide complimentary credit monitoring services as a precaution. 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 12 months 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in 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. This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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 e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

If you have questions, please contact our dedicated and confidential call center at [REDACTED]

The response line is available for 90 days from the date of this letter, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Newport News Redevelopment and Housing Authority
227 27th Street | P.O. Box 797
Newport News, VA 23607

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.