

Christine Czuprynski
Direct Dial: 248.220.1360
E-mail: cczuprynski@mcdonaldhopkins.com

December 8, 2022

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

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: City of Whitehall – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents the City of Whitehall, OH (“Whitehall”). I am writing to provide notification of an incident at Whitehall that may affect the security of personal information of forty-seven (47) Maryland residents. By providing this notice, Whitehall does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On May 27, 2022, Whitehall detected that a ransomware infection began encrypting files stored on our network. Upon learning of this issue, Whitehall contained the threat by disabling and isolating the affected systems, and immediately commenced a prompt and thorough investigation. As part of the investigation, Whitehall began working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual file review, On October 12, 2022, Whitehall discovered that the unauthorized party accessed certain files containing personal information that were maintained on the affected systems. The information potentially accessed include full name, Social Security number, and driver license number or state ID, and email address and password.

Whitehall has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Whitehall wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Whitehall is providing the affected residents with written notification of this incident commencing on or about December 8, 2022 in substantially the same form as the letter attached hereto. Whitehall is also offering the affected residents complimentary one-year membership with a credit monitoring service. Whitehall will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Whitehall will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports.

December 8, 2022

Page 2

The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Whitehall, protecting the privacy of personal information is a top priority. Whitehall is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Whitehall 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 (248) 220-1360 or cczuprynski@mcdonaldhopkins.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine Czuprynski", with a stylized flourish at the end.

Christine N. Czuprynski

Encl.



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

To Enroll, Please Call:

Or Visit:

<https://response.idx.us/city-of-whitehall>

Enrollment Code:

***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear

The privacy and security of the personal information we maintain is of the utmost importance to The City of Whitehall ("Whitehall"). We are writing with important information regarding a data security incident that involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On May 27, 2022, Whitehall detected that a ransomware infection began encrypting files stored on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling and isolating the affected systems, and immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents.

After an extensive forensic investigation and manual file review, we recently discovered that the unauthorized party accessed certain files containing personal information that was maintained on the affected systems. To date, we have no evidence that any of the information has been misused, and are not aware of any reports of identity or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

Since detecting the incident, we have reviewed and revised our information security practices, and bolstered our existing security. We are confident these actions will mitigate the chance of a future incident.

What Information Was Involved.

The impacted files contained some of your personal information, specifically your name and

What You Can Do.

We have no evidence that your information has been specifically misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary membership in identity theft protection services through IDX, the data breach and recovery services provider. IDX identity protection services include: months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on

identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary [REDACTED] membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or 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.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [REDACTED]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 9AM to 9PM Eastern time, excluding holidays.

Sincerely,

[REDACTED]

City of Whitehall

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED]-Month Credit Monitoring.

Go to <https://response.idx.us/city-of-whitehall> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. 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. Please note that the enrollment deadline is March 8, 2023.

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.

2. Placing a Fraud Alert on Your Credit File.

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
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

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

TransUnion

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

3. 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
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. 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 your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, 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.

4. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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; <https://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.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.