

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

July 14, 2022

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

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

Re: Johnson O'Hare Company, Inc. – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Johnson O'Hare Company, Inc. ("JOH"). I am writing to provide notification of an incident at JOH that may affect the security of personal information of twenty ("20") Maryland residents. JOH'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, JOH does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On June 1, 2022, JOH detected unauthorized access to its network as a result of a ransomware infection. This ransomware infection encrypted certain files stored on JOH's network. Upon learning of this issue, JOH contained the threat by disabling all unauthorized access to its network, restored all encrypted data, and immediately commenced a prompt and thorough investigation. As part of the investigation, JOH has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Though the investigation is ongoing, JOH determined on June 21, 2022 that the perpetrator may have removed certain files and folders from the network, that contain personal information. The information included the residents' full name and Social Security number.

JOH has no indication that any information has been misused. Nevertheless, out of an abundance of caution, JOH is providing notice to the affected residents commencing on July 14, 2022 in substantially the same form as the document attached hereto. JOH is offering 24 months of complimentary credit monitoring to all residents. Additionally, JOH will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. JOH will further 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. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Should you have any questions regarding this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine Czuprynski", with a stylized, flowing script.

Christine N. Czuprynski

Encl.



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[REDACTED]
[REDACTED]
[REDACTED]

July 14, 2022

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Johnson O'Hare Company, Inc. ("JOH"). We are writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident, explain 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 June 1, 2022, JOH detected unauthorized access to its network as a result of a ransomware infection. This ransomware infection encrypted certain files stored on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network, restored all encrypted data, 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. Though the investigation is ongoing, JOH determined on June 21, 2022 that the perpetrator may have removed certain files and folders from the network, that contain your information.

What Information Was Involved.

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

What You Can Do.

We have no evidence that any of your information has been 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 providing you with access to identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit monitoring 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.

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 contact [REDACTED] at [REDACTED] or [REDACTED]

Sincerely,

[REDACTED]

[REDACTED]

[REDACTED]

Johnson O'Hare Company, Inc.
1 Progress Rd,
Billerica, MA 01821

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 24-Month Credit Monitoring.

Enter your Activation Code: [REDACTED]

Enrollment Deadline: October 14, 2022

Enrollment. We encourage you to contact IDX to enroll in free identity protection services by calling [REDACTED] or going to [REDACTED] and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

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.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one (1) 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 105788

Atlanta, GA 30348

<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 LLC

P.O. Box 6790

Fullerton, CA 92834-6790

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

3. 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 charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(800) 349-9960

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000

Chester, PA 19016

<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 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.

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.

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.

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.

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

August 8, 2022

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

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

Re: Johnson O'Hare Company, Inc. – Supplemental Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Johnson O'Hare Company, Inc. ("JOH"). I am writing to provide a supplemental notification of an incident at JOH that may affect the security of personal information of one ("1") additional Maryland resident, in addition to the twenty ("20") impacted residents previously reported. JOH'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, JOH does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On June 1, 2022, JOH detected unauthorized access to its network as a result of a ransomware infection. This ransomware infection encrypted certain files stored on JOH's network. Upon learning of this issue, JOH contained the threat by disabling all unauthorized access to its network, restored all encrypted data, and immediately commenced a prompt and thorough investigation. As part of the investigation, JOH has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The investigation has concluded, on July 19, 2022 JOH discovered that the perpetrator may have removed certain files and folders from the network, that contain personal information for an additional resident. The information included the resident's full name and Social Security number.

JOH has no indication that any information has been misused. Nevertheless, out of an abundance of caution, JOH is providing notice to the affected resident commencing on August 8, 2022 in substantially the same form as the document attached hereto. JOH is offering 24 months of complimentary credit monitoring to the resident. Additionally, JOH will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. JOH will further advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free

August 8, 2022

Page 2

credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Should you have any questions regarding this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

A handwritten signature in black ink, appearing to read "Christine N. Czuprynski". The signature is fluid and cursive, with the first name "Christine" written in a larger, more prominent script than the last name "Czuprynski".

Christine N. Czuprynski

Encl.



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

August 8, 2022

The privacy and security of the personal information we maintain is of the utmost importance to Johnson O'Hare Company, Inc. ("JOH"). We are writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident, explain 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 June 1, 2022, JOH detected unauthorized access to its network as a result of a ransomware infection. This ransomware infection encrypted certain files stored on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling all unauthorized access to our network, restored all encrypted data, 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. Following the conclusion of the investigation, JOH discovered on July 19, 2022 that the perpetrator may have removed certain files and folders from the network, that contain your information.

What Information Was Involved.

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

What You Can Do.

We have no evidence that any of your information has been 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 providing you with access to identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit monitoring 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.

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 contact [REDACTED] or [REDACTED]

Sincerely,

[REDACTED]

[REDACTED]

Johnson O'Hare Company, Inc.
1 Progress Rd,
Billerica, MA 01821

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 24-Month Credit Monitoring.

Enter your Activation Code: [REDACTED]

Enrollment Deadline: October 14, 2022

Website and Enrollment. Go to [REDACTED] | [REDACTED] 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. 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.

Whether or not you choose to use the complimentary 24-month credit monitoring services, we recommend that you place an initial one (1) 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 105788
Atlanta, GA 30348

<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 LLC

P.O. Box 6790
Fullerton, CA 92834-6790

<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. 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 charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(800) 349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016

<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 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.

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.

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.

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.