McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

May 17, 2021

VIA EMAIL (consumer@ag.iowa.gov)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

Re: Osceola County – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Osceola County. I am writing to provide notification of an incident at Osceola County that may affect the security of personal information of nine hundred thirty-two (932) Iowa residents. Osceola County'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, Osceola County does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

Osceola County learned recently that an unauthorized party temporarily obtained access to a limited number of Osceola County employee email accounts between February 10, 2020 and February 27, 2020. Upon learning of this issue, Osceola County immediately secured these accounts and commenced a prompt and thorough investigation. Osceola County worked very closely with external cybersecurity professionals to perform an extensive forensic investigation and manual review of documents in these accounts. While Osceola County has no reason to believe at this time that any personal information was actually accessed, Osceola County discovered on April 2, 2021 that the compromised email accounts contained a limited amount of personal information. The information included the affected residents' full names, Social Security numbers, driver's license numbers, state identification numbers, passport numbers, bank account information, credit or debit card account information and biometric information. Not all affected residents had each of these data points impacted.

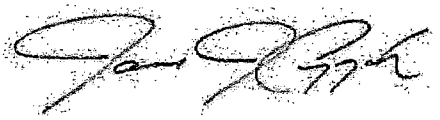
Osceola County has no evidence that any of the information has been misused. Out of an abundance of caution, Osceola County wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the impacted residents against identity fraud. Osceola County is providing the affected residents with written notification of this incident commencing on or about May 17, 2021 in substantially the same form as the letter attached hereto. Osceola County is providing the affected residents whose Social Security

numbers were impacted with 12 months of credit monitoring. Osceola County is advising the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Osceola County is also advising 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 whose financial account information was impacted are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Osceola County, protecting the privacy of personal information is a top priority. Osceola County is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Osceola County continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



James J. Giszczak

Encl.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Osceola County. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that a limited number of Osceola County employee email accounts may have been compromised by a phishing attack resulting in unauthorized access to the email boxes.

What We Are Doing.

Upon learning of the issue, we 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 document review, we discovered on April 2, 2021, that the impacted email accounts that were accessed between February 10, 2020, and February 27, 2020, contained some of your personal information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The impacted email accounts that were accessed contained some of your personal information, including your [redacted]

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one-year membership in Triple Bureau Monitoring/Report/Score provided by CyberScout. For more information on identity theft prevention, including instructions on how to activate your one-year 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. To the extent it is helpful, we have also provided information on protecting your medical information.

For More Information.

Please accept our apologies that this incident occurred. We are 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 and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our toll free response line 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, 8 am to 8 pm Central time.

Sincerely,

Osceola County

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a precautionary measure, we are providing you with; **Triple Bureau Monitoring/Report/Score,** access to a Fraud Specialist and remediation support, including $1Million in Identity Theft Expense Reimbursement Insurance, in the event you become a victim of fraud. These services will be available to you at no charge for 12 months and will begin as soon as you complete your registration. When changes occur to your Experian, TransUnion and/or Equifax credit file, notification is sent to you the same day the change or update takes place with the bureau. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

To Register your account and activate your services:

1. Type the following URL into your browser: [redacted]
2. Click the "Sign Up" button and follow the instructions to create your account.
3. Enter your information and the following Access Code to complete your registration: [redacted]
4. Next, click the "Use Now" link on the Monitoring Services tile to verify your identity and activate your monitoring services.

Important – you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

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 sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

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 monitoring 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.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

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.

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: 800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

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.