

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

April 21, 2023

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

Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Oxenham Group – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Oxenham Group. I am writing to provide notification of an incident at Oxenham Group that may affect the security of personal information of approximately three (3) Maryland residents. Oxenham Group'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, Oxenham Group does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about December 8, 2022, Oxenham Group discovered an outgoing spam email campaign that appeared to be from one of its employee email accounts. Upon discovering this, Oxenham Group's technology team acted quickly to reset passwords and ensure the security of its systems. At that time, Oxenham Group began a comprehensive review of the impacted data to determine the types of protected information that may have been exposed and to identify individuals potentially impacted by the incident. On March 23, 2023, Oxenham Group concluded its review and determined that the incident involved 3 Maryland residents. Further, on April 19, 2023, Oxenham Group located the most recent contact information for these individuals. The personal information potentially obtained included first and last name and one or more of the following: date of birth, social security number, tax ID, and bank account information.

Oxenham Group wanted to inform you (and the affected residents) of the incident and explain the steps that it is taking to help safeguard the affected residents against identity fraud. Oxenham Group is providing the affected residents with written notification of this incident commencing on or about April 24, 2023 in substantially the same form as the letter attached hereto.

Chicago | Cleveland | Columbus | Detroit | West Palm Beach

mcdonaldhopkins.com

Oxenham Group is offering the affected residents whose Social Security numbers were potentially impacted complimentary one-year memberships with a credit monitoring service. Oxenham Group is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the Maryland Attorney General's office, the consumer reporting agencies and the Federal Trade Commission.

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

Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Colin M. Battersby', with a stylized, cursive script.

Colin M. Battersby

Encl.



Re: Notice of a Data Security Incident

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to Oxenham Group, LLC ("Oxenham Group"). We're writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened?

On or about December 8, 2022, we discovered an outgoing spam email campaign that appeared to be from one of our employee email accounts. When we discovered the suspicious activity, our technology team acted quickly to reset passwords and ensure the security of our systems.

What We Are Doing.

Based on the results of our investigation, on March 23, 2023, we determined that your information was contained within the compromised email account and therefore potentially subject to unauthorized access.

What Information Was Involved.

The information involved contained your [REDACTED]

What You Can Do.

We want to make you aware of the incident and suggest steps that you should take to protect yourself.

This letter provides 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. If your bank account 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. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Finally, 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. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation 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.

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 email [REDACTED]

Sincerely,

Steven Mogle
Managing Partner
Oxenham Group, LLC
4816 S. Technopolis Drive
Sioux Falls, SD 57106

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

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 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

2. 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 30348-5788
<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.

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.

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.

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.

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 (Toll-free within North Carolina), 919-716-6000.

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