

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

June 24, 2022

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

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

Re: Dynatronics – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Dynatronics. I am writing to provide notification of an incident at Dynatronics that may affect the security of personal information of one (“1”) Maryland resident. Dynatronics’ 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, Dynatronics does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Dynatronics recently learned that two employee email accounts were accessed by an unauthorized user between December 20, 2021 and February 1, 2022. Upon learning of this issue, Dynatronics engaged third party forensic experts to review the impacted user accounts to determine the scope and extent of the incident. After an extensive forensic investigation and manual document review, Dynatronics discovered on May 25, 2022 that the impacted accounts contained a resident’s full name and health insurance information.

Dynatronics has no indication that any information has been misused. Nevertheless, out of an abundance of caution, Dynatronics is providing notice to the affected resident commencing on June 24, 2022 in substantially the same form as the document attached hereto. Additionally, Dynatronics will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Dynatronics 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 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) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,



Dominic A. Paluzzi

Encl.

Dynatronics Corporation
P.O. Box 3923
Syracuse, NY 13220



[REDACTED]

[REDACTED]

Important Information Please Review Carefully

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Dynatronics Corporation. We are writing with important information regarding a recent security incident that may have resulted in the inadvertent disclosure of your personal 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?

Dynatronics recently learned that two employee email accounts were accessed by an unauthorized user between December 20, 2021 and February 1, 2022.

What We Are Doing.

Upon learning of this issue, we immediately engaged third party forensic experts to review the impacted user accounts to determine the scope and extent of the incident. As a result of the incident, we devoted considerable time and effort to determine what information was accessible as a result of the unauthorized access.

What Information Was Involved.

After an extensive forensic investigation and manual document review we discovered on May 25, 2022 that your personal information was stored in one or more of the impacted user accounts and potentially accessible to the unauthorized user. This information contained your [REDACTED]

What You Can Do.

Please note, we have no evidence that any of your information has been misused as a result of this incident, nonetheless we are notifying you of this incident. This letter provides 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.

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, including updating passwords and enhancing email access protocols.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions 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 8:00 am to 8:00 pm Eastern, excluding holidays.

Sincerely,

[REDACTED]

Dynatronics Corporation
1200 Trapp Road,
Eagan, MN 55121

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 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 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, PA 92834-

6790
<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

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016

<https://www.transunion.com/credit-freeze>
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 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 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.

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.