

Beth Gillin
Direct Dial: 216.348.5457
E-mail: bgillin@mcdonaldhopkins.com

March 14, 2025

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

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

Re: OEC Freight Companies Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents OEC Freight Companies Inc. (“OEC Group”). I am writing to provide notification of an incident at OEC Group that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, OEC Group does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

As a result of a recent data security incident, an unauthorized party accessed and acquired certain files maintained on OEC Group computer systems. Upon detecting the unauthorized activity on or about May 13, 2024, OEC Group promptly contained the incident and commenced a thorough investigation. As part of OEC Group’s investigation, OEC Group has been working closely with external cyber security professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, OEC Group determined on February 14, 2025, that one or more of the files accessed by the unauthorized party contained a limited amount of personal information including the resident’s full name and driver’s license number.

OEC Group has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, OEC Group is providing notice to the affected resident commencing on March 14, 2025, in substantially the same form as the letter attached hereto. Additionally, OEC Group will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. OEC Group will also 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, the Federal Trade Commission and the Maryland Attorney General Consumer Protection Division and the Federal Trade Commission.

March 14, 2025

Page 2

At OEC Group, protecting the privacy of personal information is a top priority. OEC Group is committed to maintaining the privacy of the personal information entrusted to it by its affiliates and has taken many precautions to safeguard it. OEC Group 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 (216) 348-5457 or bgillin@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink that reads "Beth Gillin". The signature is written in a cursive, flowing style.

Beth Gillin

Encl.



[REDACTED]

[REDACTED]

March 14, 2025

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to OEC Freight Companies Inc. ("OEC Group"). We are writing with important information regarding a data security incident that may have involved some of your personal information. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your personal information.

What Happened?

As a result of a recent data security incident, an unauthorized party accessed and acquired certain files maintained on our computer systems.

What We Are Doing.

Upon detecting the unauthorized activity on or about May 13, 2024, we promptly contained the incident and commenced a thorough investigation. As part of our investigation, we have been working closely with external cyber security professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we determined on February 14, 2025, that one or more of the files accessed by the unauthorized party contained a limited amount of your personal information.

What Information Was Involved?

The impacted files contained your [REDACTED]

What You Can Do

We have no evidence of financial fraud or identity theft related to the impacted information. 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. 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 that it is helpful, we are also suggesting steps you can take to protect your medical information on the following pages.

For More Information

OEC Freight is committed to maintaining the privacy of personal information in our possession. 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 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 6:00 AM – 6:00 PM Pacific time, Monday through Friday, excluding holidays.

Sincerely,

OEC Freight Companies Inc.
500 Naches Ave SW Suite 100,
Renton, WA 98057

– 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. **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 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.

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.

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.

5. Protecting Your Medical Information.

The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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.marylandattorneygeneral.gov, 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; 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.