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

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

June 30, 2021

Attorney General John Formella
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: E.T. Dayton, Inc. dba Dayton Ritz & Osborne – Incident Notification

Dear Attorney General Formella:

McDonald Hopkins PLC represents E.T. Dayton, Inc. dba Dayton Ritz & Osborne ("Dayton Ritz Osborne"). I am writing to provide notification of an incident at Dayton Ritz Osborne that may affect the security of personal information of approximately two (2) New Hampshire residents. Dayton Ritz Osborne'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, Dayton Ritz Osborne does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Dayton Ritz Osborne recently learned that one Dayton Ritz Osborne employee email account was compromised by an email phishing attack resulting in unauthorized access. Upon learning of the incident, Dayton Ritz Osborne immediately secured the account and commenced a prompt and thorough investigation. After an extensive forensic investigation and manual document review, Dayton Ritz Osborne discovered on March 22, 2021 that the compromised email account contained certain elements of personal data. Thereafter, Dayton Ritz Osborne worked to identify impacted business customers, who are the data "owners." Dayton Ritz Osborne provided notice of this incident to those data owners, seeking permission to provide direct notice to individuals and requesting last known mailing addresses for impacted individuals. On May 17, 2021, Dayton Ritz Osborne learned that two impacted individuals are New Hampshire residents and obtained necessary contact information and permissions to provide those New Hampshire residents with notification. The information impacted is name and driver's license number.

To date, Dayton Ritz Osborne is not aware of any misuse of any information as a result of this incident. Nevertheless, out of an abundance of caution, Dayton Ritz Osborne wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Dayton Ritz Osborne is providing the affected residents with written notification of this incident commencing on or about June 14, 2021 in substantially the same form as the letter attached hereto. Dayton Ritz Osborne 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 consumer reporting agencies and the Federal Trade Commission.

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

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,

Christine N. Czuprynski

Encl.

E.T. Dayton, Inc. dba Dayton Ritz & Osborne
[redacted]

DAYTON RITZ +OSBORNE INSURANCE

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

June 14, 2021

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to E.T. Dayton, Inc. dba Dayton Ritz & Osborne ("Dayton Ritz Osborne"). We are writing with important information regarding a recent security incident that may have impacted some of your information. Dayton Ritz Osborne provides insurance-related services to businesses, including your current/former employer, and has access to certain personal information as a result. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized individual may have obtained access to one Dayton Ritz Osborne employee email account between October 28, 2020, and November 17, 2020.

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. We devoted considerable time and effort to determine what information was contained in the affected email account. After an extensive forensic investigation and manual document review, we learned on March 22, 2021 that the compromised email account contained certain elements of your personal data. Thereafter, we provided notice of this incident to your current or former employer, and, on May 17, 2021, obtained necessary contact information and permissions to provide you with notification. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

What Information Was Involved?

The impacted email account contained some of your personal information, specifically your name and driver's license number.

What You Can Do.

The following materials provide 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.

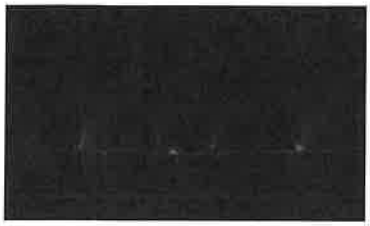
For More Information.

Please accept our sincere 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]. The response line is available Monday through Friday, 8am to 5pm Eastern time.

Sincerely,

E.T. Dayton, Inc. dba Dayton Ritz & Osborne



– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may 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 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

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.freeze.equifax.com
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
http://www.transunion.com/securityfreeze
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.

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.

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: 1-888-743-0023.

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, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.