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

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

April 23, 2021

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Entreprise Robert Thibert, Inc. – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Entreprise Robert Thibert, Inc. ("ERT"). I am writing to provide notification of an incident at ERT that may affect the security of personal information of approximately one (1) New Hampshire resident. ERT'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, ERT does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On January 25, 2021, ERT discovered that a third party obtained unauthorized access to its IT systems. As soon as it discovered the incident, ERT took the necessary measures to contain the incident and secure its infrastructure. ERT also retained the services of information technology and cybersecurity specialist firms to investigate the incident and provide it with recommendations to strengthen its security posture and prevent future threats. While ERT's investigation is still ongoing, based on the information available to date, ERT concluded on February 14th, 2021, that the attackers may have accessed its human resources directory, which contains some personal information, including: full names, banking information provided for payroll, Social Security numbers, and any other government identification documents provided to Human Resources, where applicable.

To date, there is no evidence of any misuse of personal information, nor is there any evidence that personal information will be misused in the future. Nevertheless, out of an abundance of caution, ERT 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 resident against identity fraud. ERT is providing the affected resident with written notification of this incident commencing on or about April 26th, 2021, in substantially the same form as the letter attached hereto. ERT is offering the affected resident a complimentary one-year membership with a credit monitoring service. ERT is advising the affected resident about the process for placing fraud alerts and/or security freezes 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.

At ERT, protecting the privacy of personal information is a top priority. 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,

Colin M. Battersby

Encl.

THIBERT

[redacted]

Re: Update on a Recent Incident

Dear [redacted],

As you know, our systems were recently affected by a ransomware incident. We wish to provide you with an update on the incident and on the measures put in place to respond to it.

While we are unaware of any attempted or actual misuse of any of your information, out of an abundance of caution we wanted to give you some information about the incident so that you can understand what happened, how you may be involved, the steps we have taken and some steps you can take in response.

What happened? On January 25, 2021, we discovered that a third party obtained unauthorized access to our IT systems. As soon as we discovered the incident, we took the necessary measures to contain it and secure our infrastructure. We also retained the services of information technology and cybersecurity specialist firms to investigate the incident and provide us with recommendations to strengthen our security posture and prevent future threats.

What information was involved? Based on the information available to date, the third party may have accessed a directory that contains some of your personal information. We are only notifying you of this as a precautionary measure, since there is no evidence of any misuse of your personal information, nor is there any evidence that your personal information will be misused in the future.

The information involved may include your full name, email and residential address, date of birth, banking information provided for payroll, Social Security number, and any other government identification documents provided to Human Resources, where applicable.

What can you do? While there is no evidence of actual misuse of your personal information, nor is there any evidence that such misuse will take place in the future, we encourage you to enroll in the 12 months credit monitoring services provided through TransUnion at no cost to you. These services will offer credit monitoring, email notifications to key changes to your file, Identity Theft Insurance and Dark Web Monitoring. To activate your credit monitoring account, please visit www.mytrueidentity.com and use your unique activation code [redacted] before December 31, 2021.

As a general matter and for best practice, we also encourage you to remain vigilant to phishing attempts including any risk of identity theft and fraud. There are various steps you can take to help protect your personal information including those set out below:

- protect your personal information and report any unusual activity,
- use complex passwords and change them often,
- keep your passwords in a safe place, and
- avoid opening e-mail attachments that look suspicious.

T 1 800 361 9805 | 450 691 4387
W rthibert.com

315 boulevard Industriel, Châteauguay (Québec) Canada J6J 4Z2

If you have any additional questions about this notice, please contact us by telephone at [redacted], or toll free at [redacted]. You can also contact us by [redacted]

Best regards,

[redacted]

Entreprise Robert Thibert Inc.

Other Important Information

1. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, 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	**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

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	**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
www.freeze.equifax.com	www.experian.com/freeze	www.transunion.com/securityfreeze
1-800-349-9960	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 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 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.

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.

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.

How to Sign up for *my*TrueIdentity Credit Monitoring

To help protect your identity, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at [redacted] and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

Once you are enrolled, you will be able to obtain an initial 3-in-1 credit report and credit scores along with one year of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes dark web internet identity monitoring, the ability to lock and unlock your TransUnion credit report, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply*.)

You can sign up for the *my*TrueIdentity online credit monitoring anytime between now and **on or before December 31, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, Experian, or Equifax, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

* *The Identity Theft Insurance is underwritten and administered by insurance company subsidiaries or affiliates of American International Group, Inc. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*