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

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

May 18, 2022

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Brinster & Bergman, LLP – Incident Notification

Dear Mr. Formella:

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

Brinster & Bergman was informed that some of their clients had received a letter from the IRS indicating that a tax return had been filed in their name and the IRS questioned the legitimacy of that filing, requiring the taxpayer to take certain actions. Upon learning of some of its clients receiving IRS letters, Brinster & Bergman promptly commenced an investigation of its own internal systems. As part of its investigation, Brinster & Bergman notified the IRS, changed its electronic filing identification number, changed passwords, and engaged cyber security professionals that regularly investigate and analyze these types of situations. After an extensive forensic investigation and manual document review, Brinster & Bergman discovered on April 21, 2022 that between January 10, 2022 and January 20, 2022 the unauthorized party may have obtained access to some personal information, specifically, names, SSN's and bank/financial account information.

Brinster & Bergman 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. Brinster & Bergman is providing the affected residents with written notification of this incident commencing on or about May 18, 2022 in substantially the same form as the letter attached hereto. Brinster & Bergman will offer the affected residents complimentary one-year membership with a credit monitoring service. Brinster & Bergman will advise the affected

residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Brinster & Bergman will advise the affected residents about the process for placing a fraud alert and/or security freeze 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 Brinster & Bergman, protecting the privacy of personal information is a top priority. Brinster & Bergman is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Brinster & Bergman continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

James J. Giszczak

Brinster & Bergman, LLP
Return Mail Processing Center
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

Brinster & Bergman, LLP
CERTIFIED PUBLIC ACCOUNTANTS

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [redacted]

[redacted]

[redacted]

May 18, 2022

Dear [redacted]

The privacy of your personal information is of utmost importance to Brinster & Bergman, LLP. In light of the ongoing cyber security threats to the accounting industry, especially this year, we are writing to provide you with important information regarding recent IRS correspondence that some of our clients have received. We also wanted to provide you with details about the forensic investigation we conducted of our systems, explain the services we are making available to help safeguard you against identity fraud and provide additional steps you can take to further protect your information.

What Happened?

Some of our clients have recently informed us that they have received a letter from the IRS indicating that a tax return had been filed in their name and the IRS questioned the legitimacy of that filing, requiring the taxpayer to take certain actions. For those clients who have notified us of these letters, we have worked with them to paper file their returns, along with Form 14039 (Identity Theft Affidavit). If you have received an IRS letter and have not notified our office yet, please do so immediately so that we can take the necessary steps on your behalf. You do NOT need to respond to the IRS directly; we will handle that for you.

What We Are Doing.

Upon learning of some of our clients receiving IRS letters, we promptly commenced an investigation of our own internal systems. As part of our investigation, we notified the IRS, changed our electronic filing identification number, changed passwords, and engaged cyber security professionals that regularly investigate and analyze these types of situations. After an extensive forensic investigation and manual document review, we discovered on April 21, 2022 that between January 10, 2022 and January 20, 2022 the unauthorized party may have obtained access to some of your personal information.

What Information Was Involved.

As you know, in connection with providing you with tax consulting services, our systems contain your name, Social Security number, and financial account information (to the extent you have provided it to us prior to January 10, 2022).

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary membership in identity theft protection services through IDX, the data breach and recovery services provider. IDX identity protection services include: [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides other 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.

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 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, 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

Brinster & Bergman, LLP

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is [redacted].

Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary credit monitoring services, you may place an initial 90-day "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

3. 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. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

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

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies' websites to find out the specific costs applicable to the State in which you currently reside.

If you decide to place a Security Freeze on your credit file, *in order to do so without paying a fee*, you will need to send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services.

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. After you sign up for the credit monitoring service, you may refreeze your credit file. We encourage you to wait to place a security freeze on your credit file until you have enrolled in the credit monitoring service to avoid paying additional fees related to placing an initial security freeze on your credit file, temporarily lifting or removing the security freeze and subsequently refreezing your credit file.

4. 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.

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.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were [redacted] Rhode Island residents impacted by this incident.