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

**Dominic A. Paluzzi**
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com



April 22, 2020

**VIA U.S. MAIL**

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

**Re: Sanborn-Tuepker Associates, P.C. – Incident Notification**

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Sanborn-Tuepker Associates, P.C. ("Sanborn"). I am writing to provide notification of an incident at Sanborn that may affect the security of personal information of approximately sixteen (16) New Hampshire residents. Sanborn'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, Sanborn does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

An unauthorized party may have obtained access to a Sanborn employee's email account, as a result of an email phishing incident. Upon learning of the issue, Sanborn secured the account and commenced a prompt and thorough investigation. As part of its investigation, Sanborn has worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, Sanborn determined on March 26, 2020 that the impacted email account that was accessed on January 28, 2020 contained a limited amount of personal information, including the affected residents' full names and Social Security numbers, and may have also included financial account information.

To date, Sanborn has no evidence that any of the information has been acquired or misused. Nevertheless, out of an abundance of caution, Sanborn 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. Sanborn will provide the affected residents with written notification of this incident commencing on or about April 22, 2020 in substantially the same form as the letter attached hereto. Sanborn will offer the affected residents complimentary one-year memberships with a credit monitoring service. Sanborn will advise 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 whose financial account information was impacted will be advised to contact their financial institutions to inquire about steps to take to

protect their accounts. The affected residents will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Sanborn, protecting the privacy of personal information is a top priority. Sanborn is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Sanborn continually evaluates and modifies its practices and internal controls to secure personal information. Since this incident, Sanborn has implemented multi-factor authentication on its email.

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.

**Sanborn-Tuepker Associates, P.C.**

[redacted]

[redacted]

Dear [redacted]

I am writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Sanborn-Tuepker Associates, P.C. ("Sanborn"). We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

*What Happened?*

An unauthorized party may have obtained access to a Sanborn employee's email account, as a result of an email phishing incident.

*What We Are Doing.*

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we determined on March 26, 2020 that the impacted email account that was accessed on January 28, 2020 contained some of your personal information. We have no evidence that any of the information has been acquired or misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

*What Information Was Involved?*

The email account that was accessed contained some of your personal information, including your [redacted]

*What You Can Do.*

To protect you from potential misuse of your information, we are offering you a one-year membership for myTrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. myTrueIdentity serves to both monitor credit and provides identity protection, alerting members any time a credit file changes. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your one-year membership, please see the additional information provided in this letter.

Also provided in "Other Important Information" are 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*.

We regret any inconvenience that this may cause you. 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 secure personal information. Since this incident, we have implemented multi-factor authentication on our email.

**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, [redacted]

Sincerely,

Sanborn-Tuepker Associates, P.C.

## – OTHER IMPORTANT INFORMATION –

### 1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) 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 to the myTrueIdentity 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.

You can sign up for the online credit monitoring service anytime between now and [redacted] Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program 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. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the toll-free TransUnion Fraud Response Services hotline at [redacted] When prompted, enter the following 6-digit telephone pass code [redacted] to speak to a TransUnion representative about your identity theft issue.

### 2. Placing a Fraud Alert on Your Credit File.

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 |

### 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, 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 |
| https://www.freeze.equifax.com | http://experian.com/freeze | http://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.

**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. 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(s) to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain new account number(s).