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
dpaluzzi@mcdonaldhopkins.com



February 13, 2018

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

**Re: Abeles & Hoffman P.C. – Incident Notification**

Dear Attorney General Delaney:

McDonald Hopkins PLC represents Abeles & Hoffman P.C. ("Abeles & Hoffman"). I write to provide notification concerning an incident that may affect the security of personal information of one (1) New Hampshire resident. Abeles & Hoffman's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Abeles & Hoffman does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Abeles & Hoffman recently learned that a limited number of email users were victims of a spear-phishing attack resulting in unauthorized access to those users' email boxes between September 26-28, 2017. Upon learning of the issue, Abeles & Hoffman promptly responded to the incident, reset log-in credentials and implemented multi-factor authentication for all email accounts. In addition, an independent cybersecurity forensic firm was engaged to analyze the incident and the extent of any compromise to the email accounts.

After an extensive manual email review, which was concluded on January 18, 2018, Abeles & Hoffman confirmed that the impacted email accounts that were accessed contained some personal information, including full name and Social Security number. Although some personal information was contained within the accessed email account, Abeles & Hoffman had no evidence that personal information was actually accessed, viewed, downloaded or otherwise acquired by a potential unauthorized user.

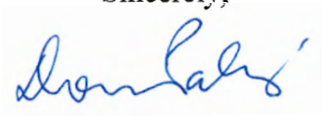
To date, Abeles & Hoffman is not aware of any confirmed instances of identity fraud as a direct result of this incident. Nevertheless, Abeles & Hoffman wanted to make you (and the affected resident) aware of the incident and explain the steps Abeles & Hoffman is taking to help safeguard the resident against identity fraud. Abeles & Hoffman provided the New Hampshire resident with written notice of this incident commencing on February 13, 2018, in substantially the same form as the letter attached hereto. Abeles & Hoffman is offering the resident a complimentary membership with a credit monitoring and identity theft protection service. Abeles & Hoffman has advised the resident to remain vigilant in reviewing financial account statements

for fraudulent or irregular activity. Abeles & Hoffman has advised the resident about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The resident also has been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Abeles & Hoffman is committed to maintaining the privacy of personal information and have taken many precautions to safeguard it. Abeles & Hoffman continually evaluates and modifies its practices to enhance the security and privacy of personal information, including the encryption of all outgoing mail to help prevent similar issues in the future.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.

ABELES AND HOFFMAN P.C.
CERTIFIED PUBLIC ACCOUNTANTS AND BUSINESS CONSULTANTS

Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

[redacted]

***IMPORTANT INFORMATION***
***PLEASE READ CAREFULLY***

[redacted]

Dear [redacted]:

The privacy of your personal information is of utmost importance to Abeles and Hoffman P.C. We are writing to provide you with important information about a recent incident involving some of your personal information that is maintained by us, along with the services we are making available to help safeguard your information.

We recently learned that a limited number of email users were victims of a spear-phishing attack resulting in unauthorized access to those users' email boxes between September 26-28, 2017. Upon learning of the issue, we promptly responded to the incident, reset log-in credentials and implemented multi-factor authentication for all email accounts. In addition, an independent cybersecurity forensic firm was engaged to analyze the incident and the extent of any compromise to the email accounts.

After an extensive manual email review, which was concluded on January 18, 2018, we can confirm that the impacted email accounts that were accessed contained some of your personal information, including your full name and Social Security number. Although some of your personal information was contained within the accessed email account, we have no evidence that your personal information was actually accessed, viewed, downloaded or otherwise acquired by a potential unauthorized user.

**To date, we are not aware of any reports of identity fraud, theft, or improper use of personal information as a direct result of this incident.** To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorks$^{SM}$ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter. Also enclosed in this letter, you will find information about 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 obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of personal information and we have taken many precautions to help safeguard it, including the encryption of all outgoing email. 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 help protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

[redacted]

Abeles and Hoffman P.C.

## – ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

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

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks[SM] Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

**Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll [redacted]
3. PROVIDE the **Activation Code**: : [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted]. Be prepared to provide [redacted] as proof of eligibility for the identity restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [redacted]**
**or call [redacted] to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted].

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## 2. 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 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
www.equifax.com
1-800-525-6285

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

**TransUnion**
P.O. Box 2000
Chester, PA 19016
www.transunion.com
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. 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**
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

**Experian Security Freeze**
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

**TransUnion Security Freeze**
P.O. Box 2000
Chester, PA 19022
http://www.transunion.com/securityfreeze
1-800-680-7289

## 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.

**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.

**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.

**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.

**6. Reporting Identity Fraud to the IRS.**

If you believe you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police or law enforcement department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

**7. Reporting Identity Fraud to the Social Security Administration.**

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.