100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

McDonald Hopkins

A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

August 23, 2022

VIA U.S. MAIL
Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Breach Notification

To Whom It May Concern,

We are writing on behalf of our client, Abeles and Hoffman, P.C. ("Abeles and Hoffman") (located at 9666 Olive Blvd., St. Louis, MO 63132) to notify you of a data security incident involving five (5) New Hampshire residents.[1]

Nature

On August 24, 2021, Abeles and Hoffman discovered that an unauthorized individual gained access to one of its email accounts and began a spam campaign. After discovering the incident, Abeles and Hoffman quickly took steps to secure and remove the access from the email accounts. Further, Abeles and Hoffman immediately engaged independent third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in remediation efforts. On October 27, 2021, the forensic investigation concluded and found that the unauthorized individual likely used a phishing email to gain access. Abeles and Hoffman believes the intent was to launch a spam campaign and or commit financial fraud (which did not occur).

At that time, Abeles and Hoffman began a comprehensive review of the information that might be involved. Abeles and Hoffman recently concluded its review and, on August 8, 2022, determined that the incident involved personal information related to five (5) New Hampshire residents.

The personal information included first and last names, dates of birth, social security numbers, driver's license numbers, credit card numbers, passport numbers, financial account and routing numbers, medical information, and health insurance information.

[1] By providing this notice, Abeles and Hoffman does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

However, as of now, we have no evidence indicating financial fraud or identity theft of any of the information.

Notice and Abeles and Hoffman's Response to the Event

On August 23, 2022, Abeles and Hoffman will mail a written notification to the potentially affected New Hampshire residents, pursuant to N.H. Rev. State § 359-C:19, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Abeles and Hoffman is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Cyberscout;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Finally, Abeles and Hoffman is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

Abeles and Hoffman P.C
P.O. Box 3923
Syracuse, NY 13220

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

9666 Olive Blvd.
St. Louis, MO 63132
314-991-4770

[redacted]

August 23, 2022

Re: Notice of a Data Security Incident

Dear [redacted]

At Abeles and Hoffman, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involved your personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened

On August 24, 2021, we discovered that an unauthorized individual gained access to one of our employee email accounts and began a spam campaign. After discovering the incident, we quickly took steps to secure and remove unauthorized access from our email accounts. Further, we engaged independent third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and to assist in remediation efforts. At the conclusion of the forensic investigation, we determined that, on or about July 29, 2021, an unauthorized individual likely accessed and obtained some information from one of our employee email accounts as a result of the incident.

At that time, we began a comprehensive review of the information that might have been obtained by the unauthorized individual. We recently concluded our full review of the impacted information and determined that it included some of your personal information. ***However, as of now, we have no evidence indicating identity theft or financial harm involving any of your information.*** Regardless, we wanted to notify you of the incident out of an abundance of caution and provide you information on how to best protect yourself from identity theft and fraud.

What Information Was Involved

The personal information could potentially involve [redacted].

What We Are Doing

As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating identity theft or financial harm involving any of your information in connection with this incident, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. In addition, please see "***OTHER IMPORTANT INFORMATION***" on the following pages for guidance on how to best protect your identity.

In response to the incident, we are providing you with access to the following services:
Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of [redacted], Monday through Friday. Please call the help line [redacted] and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Finally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Additionally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

For More Information
We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have additional questions, please contact [redacted] by calling [redacted] or writing to us at [redacted].

Sincerely yours,

Justin Reppy, Principal

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION

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 (1) 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 30348-5069
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

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 30348-5788
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

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 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.

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.

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: 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, Consumer Protection Division, 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. **Washington D.C. Residents**: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.