BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Gerald J. Ferguson
direct dial: 212.589.4238
gferguson@bakerlaw.com

August 27, 2021

VIA EMAIL (DOJ-CPB@DOJ.NH.GOV)

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

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, McNair & Company ("McNair") to notify your office of a cybersecurity incident. McNair is located at 1410 Springhill Rd., Suite 400 McLean, VA 22102.

McNair recently completed an investigation that involved unauthorized access to an employee's email account. Upon discovering the incident, McNair immediately took steps to secure its email environment. A cybersecurity firm was engaged to assist with the investigation and determined that an unauthorized party was able to access the employee's email account between April 27, 2021 and May 12, 2021.

The investigation was not able to determine which emails or attachments, if any, were viewed by the unauthorized party. Therefore, McNair conducted a thorough review of the contents of the email account to identify the specific individuals whose information was contained within the emails and attachments. It was determined, on August 14, 2021 that the names, Social Security numbers, driver's license numbers, passport numbers, tax identification numbers, limited health information and/or financial account numbers for McNair's customers, former customers or beneficiaries of policies issued by McNair may have been accessed.

On August 27, 2021, McNair mailed notification letters to the individuals whose information was contained in the email account, including 1 New Hampshire resident[1]. A copy of the notification letter is enclosed. McNair is offering a complimentary one-year membership in credit monitoring and identity theft protection services through Kroll to the notified individuals. McNair also established a dedicated call center for individuals to call with questions about the incident or enrolling in the credit monitoring services.

To reduce the risk of a similar incident occurring in the future, McNair implemented additional measures to further enhance the security of its network and existing security protocols.

Please do not hesitate to reach out with any questions.

Sincerely,

Gerald J. Ferguson
Partner

Enclosure

[1] This notice does not waive McNair's objection that New Hampshire lacks personal jurisdiction over it regarding any claims relating to this incident.

McNAIR
& COMPANY
Since 1931

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<last_name>>,

McNair & Company recognizes the importance of protecting personal information. We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken in response, and some additional steps you may consider taking.

We recently completed an investigation that involved unauthorized access to an employee's email account. Upon discovery of the incident on May 12, 2021 we immediately took steps to secure our email environment and begin an investigation. A cybersecurity firm was engaged to assist with the investigation and determined that an unauthorized party was able to access the employee's email account between April 27, 2021 and May 12, 2021.

The investigation was not able to determine which emails or attachments, if any, were viewed by the unauthorized party. Therefore, we conducted a thorough review of the contents of the email account to determine the specific individuals whose information was contained within the emails and attachments. We analyzed the results and determined that an email or attachment in the account included some of your information. The information that may have been accessed could include your name, Social Security number, driver's license number, passport number, tax identification number and/or financial account number. If you provided information regarding a medical diagnosis or treatment provided in conjunction with provision of insurance or estate planning services, that information may have also been accessed.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. As a precaution, we are offering a complimentary one-year membership in Kroll's Identity Monitoring services. This service includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration and will be completely free to you. Activating these services will not hurt your credit score. For more information on Kroll's Identity Monitoring services, including instructions on how to activate your complimentary membership, and more information on identity theft prevention, please see the additional information provided with this letter.

To help prevent something like this from happening in the future, we have implemented additional measures to enhance our existing security protocols. We regret this incident occurred and apologize for any inconvenience.

If you have any questions, please call 1-???-???-???? Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Frederick V. McNair IV

Frederick V. McNair, IV
President/CEO

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***November 25, 2021*** to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission,* Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

McNair & Company 1410 Springhill Rd., Suite 400 McLean, VA 22102 (703) 448-8848

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.