

RECEIVED

OCT 07 2019

CONSUMER PROTECTION

Gregory J. Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

October 4, 2019

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Berman McAleer, LLC with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the possible security breach or unauthorized use or access

On August 21, 2019, computer experts determined that an unknown third party could have viewed personal information in the email account of a Berman McAleer employee that showed signs of being briefly accessed without authorization. During an investigation of the email account, computer experts found evidence suggesting that the unknown third party accessing the account was attempting (unsuccessfully) to intercept a wire payment. Experts saw no indication that any other employee email accounts were accessed without authorization and found no evidence that Berman McAleer's computer systems, databases or servers were accessed without authorization. At this time, Berman McAleer is not aware of any specific access to or misuse of anyone's personal information that was stored in the email account. Nonetheless, Berman McAleer reviewed the full contents of the email account and is notifying anyone whose personal information, including name, Social Security number, bank account number or driver's license number, was in the employee's mailbox and could have been exposed.

2. Number of New Hampshire residents potentially affected

Approximately one (1) New Hampshire resident was affected in this potential incident. Berman McAleer sent the potentially impacted individual a letter notifying him or her of this incident on October 4, 2019. A copy of the notification that was sent to the potentially impacted individual is included with this letter, which informs this New Hampshire resident about the 12 months of credit monitoring and identity theft protection services that is being offered to him or her.

3. Steps Berman McAleer has taken relating to the potential incident

Upon learning of this issue, Berman McAleer took steps to determine the extent of information in the account that was at risk and took steps to identify anyone potentially impacted by this incident. Berman

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

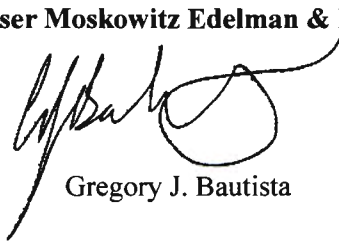
McAler has also taken steps to prevent a similar event from occurring in the future, including reviewing and revising its information security policies and procedures and resetting employees' access credentials to ensure its systems are secure.

4. Other notification and contact information

If you have any additional questions, please contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista



MARYLAND
9690 Deereco Road
Suite 800
Timonium, MD 21093
410.560.9960

NEW YORK
475 Park Avenue South
Suite 2100
New York, NY 10016
212.379.4056

«Envelope_Name»
«Primary_Street» «Primary_Street_2»
«Primary_City», «Primary_State» «Primary_Zip»

October 2, 2019

Dear «Informal_Name»,

We are sending you this letter as follow-up to the email we sent you in July regarding an unauthorized phishing email that was sent from the email address of a Berman McAleer employee. As our client, we take the security of your information very seriously and want to do all that we can to help you protect your information.

What Happened

On July 11, 2019, we discovered that a phishing email had been sent from an employee's email account to individuals outside of Berman McAleer. We immediately took steps to notify potential recipients of the phishing email and warn them not to provide their usernames or passwords if requested. We simultaneously reset the access privileges to all Berman McAleer employee email accounts. In addition, we engaged computer experts to determine how the phishing email was distributed and whether our systems were at risk. *During the investigation, experts found no indication that our computer systems, databases, or servers were accessed by an unauthorized third party and found no evidence of any malicious software in our environment.*

As a further precaution, we engaged experts to investigate potential unauthorized access to the email accounts of our employees. The investigation determined that the email account from which the phishing email was sent may have been briefly accessed by an unauthorized third party. Computer experts saw no indication that any other employee email accounts were accessed. The investigation found evidence suggesting that the unknown third party accessing the account was attempting (unsuccessfully) to intercept a wire payment.

What Information Was Involved

At this time, we are not aware of any access to or misuse of anyone's personal information that may have been stored in the email account. Nonetheless, out of an abundance of caution, we are notifying you that your information, including Social Security number, bank account information or driver's license number may have been exposed. Therefore, as an added precaution, we are providing you with resources you can use to help you protect your information.

What We Are Doing

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.

www.bmcplanning.com

What You Can Do

While your information may not be at risk, we welcome you to take advantage of this service offering. You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code «**Activation_Code**» and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode «**Telephone_passcode**» and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and January 31, 2020. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services 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.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- 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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

For More Information

We genuinely appreciate the trust you have placed in us and want to assure you that we are committed to continuously enhancing the security of our systems. Should you have any questions or concerns, please contact me at (410) 560-9960.

Sincerely,



David Berman
Co-Founder & Chief Executive Officer
Berman McAleer

Additional Important Information

For residents of Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Maryland, Missouri, and North Carolina: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Maryland, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

For residents of MA: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The contact information for all three credit bureaus is below:

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission.

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