



RECEIVED

APR 08 2019

CONSUMER PROTECTION
James P. Miller
Attorney at Law
Jim.Miller@ofplaw.com
Direct – (703) 218-2154

April 5, 2019

VIA EMAIL (attorneygeneral@doj.nh.gov)

AND FEDEX #7749 0100 5221

The Honorable Gordon J. MacDonald
Attorney General of the State of New Hampshire
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: System Security Incident

Dear Attorney General MacDonald:

We are writing on behalf of our client, The Mosaic Tile Company of Virginia, Inc. (“Mosaic”), to notify you of a system security incident affecting the personal information of one New Hampshire resident. On February 6, 2019, Mosaic discovered that an unknown, unauthorized individual may have accessed a Mosaic employee’s email account through a suspected phishing attack. Mosaic promptly secured the email account and engaged its internal Information Technology Department, with additional assistance from its Human Resources Department personnel, to determine what personal information the unknown, unauthorized individual may have accessed and acquired. After a thorough investigation that concluded on approximately March 11, 2019, and which included an exhaustive review of user email logs, email traffic information from both internal and third-party email monitoring services, and a review of all emails that were contained in the account currently and recovered from archives of deleted emails, Mosaic determined that the unknown, unauthorized individual accessed and acquired the personal information of one New Hampshire resident. The personal information included the affected person’s name, Social Security number, and driver’s license number as contained in IRS Form W-9 and/or IRS Form 1099-MISC documents. Beginning April 8, 2019, Mosaic is providing written notice via postal mail to the one New Hampshire resident affected by the system security incident in substantially the same form as the attached letter.

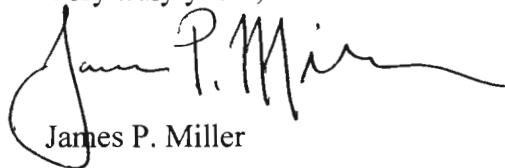
As described in the attached letter, Mosaic has established a telephone number that affected persons may call for further information and assistance, and is advising the affected persons to remain vigilant by reviewing account statements and monitoring free credit reports. Additionally, Mosaic is providing the affected persons with information on how to better protect against identity theft and fraud, including information about fraud alerts, security freezes, and contacting the Federal Trade Commission, Internal Revenue Service, Office of the Attorney

The Honorable Gordon J. MacDonald
Attorney General of the State of New Hampshire
New Hampshire Department of Justice
April 5, 2019
Page 2

General, and law enforcement to report attempted or actual identity theft and fraud. Protecting personal information is a priority of Mosaic, and Mosaic has implemented additional security measures, including further employee training and information system controls, designed to prevent a recurrence of such an attack and protect personal information from further unauthorized access and acquisition.

If you would like any additional information concerning the system security incident, please feel free to contact me at your convenience.

Very truly yours,

A handwritten signature in black ink, appearing to read "James P. Miller". The signature is fluid and cursive, with a large initial "J" and "M".

James P. Miller

Attachment

cc: The Mosaic Tile Company of Virginia, Inc.
Lauren Friend McKelvey, Esq.

#4246897v1 005855/098833

ATTACHMENT

[DATE]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE, AND POSTAL CODE]

Re: Data Security Incident

Dear [INDIVIDUAL NAME]:

We value your services to Mosaic and respect the privacy of your information, which is why, as a precautionary measure, we are writing to inform you of a data security incident that involves your personal information.

On February 6, 2019, Mosaic's Information Technology (IT) personnel identified suspicious email activity. Mosaic's internal IT Department personnel immediately commenced an investigation of the activity, promptly secured the impacted email account to ensure that emailed information was no longer being compromised, and with the help of members of our Human Resources Department, researched the impacted email account to determine the information that the unauthorized person may have accessed or obtained without authorization. This process included an exhaustive review of user email logs, email traffic information from both internal and third-party email monitoring services, and a review of all emails that were contained in the account currently and recovered from archives of deleted emails. As a result of this investigation, we believe an unauthorized individual gained access to only one Mosaic email account through the use of a phishing attack.

On approximately March 11, 2019, after the review of the email and data logs for the compromised account was completed, Mosaic determined the following personal information was impacted:

- Individual's Social Security number
- Individual's first and last name
- Individual's driver's license number
- IRS Form W-9 and/or IRS Form 1099-MISC containing the above personal information

Mosaic values your privacy and deeply regrets that this incident occurred. We have implemented additional security measures, including further employee training and information system controls, designed to prevent a recurrence of such an attack, and to protect the privacy of Mosaic's valued vendors and customers as well as our employees. For further information and assistance, please contact Tiffany Houston at 703-880-9932.

Very respectfully,

Michael D. Rockefeller
Chief Financial Officer

Steps you can take to further protect your information:

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/cra/requestformfinal.pdf. If you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374

Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626

TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338).

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You may need to separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

You may also wish to consult Internal Revenue Service resources about tax-related identity theft prevention, detection, and victim assistance: <https://www.irs.gov/identity-theft-fraud-scams>