BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

February 8, 2022

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John M. 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, Millenia Investments, LLC ("Millenia") to notify your office of a security incident involving two (2) New Hampshire residents.

Millenia experienced a data incident involving unauthorized access to an employee's email account. Millenia took steps to secure its email environment and began an investigation. An outside cybersecurity firm was engaged to assist. The investigation determined that an unauthorized individual accessed a Millenia employee's email account, but we were unable to determine the exact period of unauthorized access or which emails or attachments, if any, were viewed by the unauthorized party. Therefore, we conducted a thorough review of the entire contents of the account to determine the specific individuals whose information was contained within the emails and attachments. While Millenia has no evidence that any information was stolen or misused, the affected computer and email account may have contained personal information, including names, Social Security numbers, and financial account numbers.

On November 12, 2021, the investigation determined an unauthorized person accessed files and folders that contained personal information. Millenia then worked to identify the individuals whose information was accessed as a result of the incident.

On February 7, 2022, Millenia started mailing notification letters to the New Hampshire residents via U.S. mail in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of the notification letter is enclosed. Millenia is providing a telephone number for potentially affected

[1] This report is not, and does not constitute, a waiver of Millenia's objection that New Hampshire lacks personal jurisdiction over the company related to this matter.

individuals to call with any questions they may have about the incident. Millenia is offering notified individuals complimentary one-year memberships to identity monitoring services.

To help prevent this type of incident from happening again, Millenia is implementing additional security safeguards and further enhancing its already exiting security protocols.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

M. Scott Koller

M. Scott Koller
Partner

Enclosure

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

February 4, 2022

Dear <<Name1>><<Name 2>>:

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, and provides additional steps you may consider taking.

What Happened?
On July 13, 2021, Millenia launched an investigation into suspicious activity originating from an employee's email account. As soon as we became aware of the activity, we took immediate steps to secure the email account and a cybersecurity firm was engaged to assist in a forensic analysis of the incident. Our investigation determined that an unauthorized individual accessed a Millenia employee's email account. We were unable to determine the exact period of unauthorized access or which emails or attachments, if any, were viewed by the unauthorized party. Therefore, we conducted a thorough review of the entire contents of the account to determine the specific individuals whose information was contained within the emails and attachments.

What Information Was Involved?
We analyzed the results and on November 12, 2021, determined that an email or attachment in the account included some of your information, including your <<insert variable text>>.

What We Are Doing.
Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect your information, we have implemented additional measures to enhance our existing security protocols and are re-educating our staff for awareness on these types of incidents. Additionally, we are offering you a complimentary one-year membership in identity theft protection services through IDX. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. Please note the deadline to enroll is May 4, 2022.

What You Can Do.
We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity over the next 12 to 24 months. If you see unauthorized charges or activity, please contact your financial institution immediately. For more information, including some additional steps you can take to help protect your information, please see the pages that follow this letter.

For More Information.
We regret this incident occurred and apologize for any inconvenience. If you have any questions, please call 1-833-903-3648, Monday through Friday, 8:00 a.m. to 8:00 p.m., Central Time.

Sincerely,

Stephen A. Serati

Stephen A. Serati
President, Registered Principal
Millenia Investments, LLC

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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.

Millennia Investments, LLC is located at 16100 Chesterfield Pkwy W, Chesterfield, MO 63017.

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, 1-518-474-8583 / 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.