Appendix

New York City Management, LLC ("NYCM") recently completed an investigation that involved suspicious activity originating from two NYCM employee email accounts. Upon learning of the incident, NYCM immediately took measures to secure the accounts and launched an investigation. A third-party computer forensic firm was engaged to assist. The investigation was unable to determine which emails or attachments in the accounts were viewed by the unauthorized person. In an abundance of caution, NYCM reviewed the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person. On December 4, 2020, NYCM determined that an email or attachment in the accounts contained the name and financial account number belonging to one resident of Maine.

Today, February 17, 2021, NYCM will mail a notification letter via First Class U.S. mail to the one Maine resident.[1] NYCM has established a dedicated phone number that the individual may call with related questions.

To reduce the risk of a similar incident occurring in the future, NYCM implemented additional authentication measures for remote email access and provided further education to its staff for awareness on these types of incidents.

[1] This notice does not waive NYCM's objection that Maine lacks personal jurisdiction over it regarding any claims related to this incident.

NEW YORK CITY
NYCM
MANAGEMENT LLC

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

At NYCM, we recognize the importance of protecting personal information. We are writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking.

We recently completed an investigation into suspicious activity originating from two NYCM employee email accounts. As soon as we became aware of the activity, we immediately took measures to secure the accounts and launched a thorough investigation. A third-party computer forensic firm was engaged to assist.

The investigation determined that there was unauthorized access to the accounts between July 8, 2020 and July 27, 2020. However, the investigation was unable to determine which emails or attachments in the accounts were viewed by the unauthorized person. In an abundance of caution, we reviewed the emails and attachments that may have been viewed to identify individuals whose information may have been accessible to the unauthorized person. On December 4, 2020, we determined that an email or attachment included your <<b2b_text_1(DataElements)>>.

We believe that the unauthorized access occurred as part of an attempt to obtain money from NYCM through a wire transfer and not to access personal information. Although we do not know that your information was viewed or acquired, and we have no indication that your information has been misused, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. For more information on identity theft prevention and steps you can take to help protect your personal information, please see the attached additional information provided in this letter.

We regret any concern this incident may cause. To improve our security, we have implemented additional authentication measures for remote email access and provided further education to our staff for awareness on these types of incidents. If you have any questions, please call 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Sachin Narvekar
Controller
NYCM

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. 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.

NYCM's mailing address is 13 West 38th Street, 4th Floor, New York, New York 10018, and the phone number is (347) 650-3902.

Additional information for residents of the following states

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