North Hill
VIBRANT LIVING FOR PEOPLE AGE 65+

February 15, 2024

Consumer Protection Bureau, Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Breach

To Whom It May Concern:

This letter serves as the notification on behalf of North Hill Communities, Inc., North Hill Home Health Care, Inc., North Hill Needham, Inc., Connected for Life, Inc., and the North Hill Employee Dental Plan (collectively, "North Hill"), a senior living provider that offers home health care and continuing care services, located in Needham, Massachusetts, of a recent data breach that potentially impacted the personal information of forty-two (42) New Hampshire residents, resulting from a ransomware attack on North Hill. The potentially impacted personal information may include:

o

d

On December 26, 2023, North Hill detected a cybersecurity incident affecting certain systems in our network environment. North Hill immediately secured the network and engaged third party information technology and forensic specialists to assist with restoring systems and investigating the extent of the unauthorized activity. The forensic investigation revealed that an unauthorized party gained access to North Hill's network on December 19, 2023. After a comprehensive forensic investigation and extensive document review conducted by Arctic Wolf, North Hill was able to determine that certain data, including personal information, from the affected systems may have been accessed or acquired by the unauthorized party.

North Hill's forensic investigation was unable to conclude what specific information may have been accessed or acquired by the unauthorized party; however, it revealed that, on December 19, 2023, a threat actor gained access to North Hill's systems using a brute force attack. The Arctic Wolf forensic analysis determined that the threat actor exfiltrated approximately 50 gigabytes of data, which includes data on skilled nursing residents, home health agency patients, and participants in North Hill's self-insured dental plan. North Hill and Arctic Wolf were not able to identify with specificity which files were exfiltrated, and therefore, out of an abundance of caution, North Hill determined that it would provide notice to all of its current residents and, when applicable, next of kin, current and former employees, and employees and their dependents that are currently enrolled in the dental plan whose data was stored on North Hill's system.

On February 14, 2024 through February 16, 2024, North Hill will notify potentially impacted individuals, including the forty-two (42) New Hampshire residents of the breach to ensure transparency and awareness of our findings. A sample of the notification provided to potentially impacted individuals is attached hereto.

As a result of the incident, the malware encrypted many servers. However, North Hill was able to restore its servers using back-ups, experiencing no known loss of data, and quickly bring all services back online within four (4) days following the ransomware attack. All electronic functions were operationalized quickly and are fully functional. Once the organization became aware of the cyberattack, it implemented a number of processes to allow for continued operations. Importantly, the electronic health records system that North Hill uses to provide skilled nursing and home health care was not impacted by the attack, and healthcare services provided by North Hill remained uninterrupted. North Hill's Office 365 application also was not impacted by the attack.

In order to help protect the information of potentially impacted individuals, North Hill has taken the following steps:

- North Hill will cover the cost for for potentially impacted individuals to receive credit monitoring from Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.
- Added additional computer security protections and protocols to ensure that personal information is protected from unauthorized access;
- Notified the Federal Bureau of Investigation of this incident;
- Notified the U.S. Department of Health and Human Services of this incident, as well as other regulatory agencies; and
- Posted notice on its website to ensure that all potentially impacted individuals are aware of the breach.

North Hill understands the importance of safeguarding personal information and takes that responsibility very seriously. North Hill will do all it can to assist any individuals whose personal information may have been compromised and help them work through the process.

If you have any additional questions about this incident, please contact North Hill at Susan Downey, Director of Healthcare Services/Interim Corporate Compliance Officer at or

Sincerely,

Joseph A. Frias
President and Chief Executive Officer
North Hill Communities, Inc.
Attachments (Sample Individual Notification Letters)

North Hill Communities Inc.
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08461 1-1

[redacted]

February 14, 2024

Dear [redacted]

On behalf of North Hill Communities, Inc., North Hill Home Health Care, Inc., North Hill Needham, Inc., Connected for Life, Inc., and the North Hill Employee Dental Plan (collectively, "North Hill"), we are sending this letter to you as part of our commitment to the privacy of our community. We take the security of our residents, employees, and dental plan participants very seriously.

What Happened
On December 26, 2023, North Hill detected a cybersecurity incident affecting certain systems in our network environment. North Hill immediately secured the network and engaged third party information technology and forensic specialists to assist with restoring systems and investigating the extent of the unauthorized activity. The forensic investigation revealed that an unauthorized party gained access to North Hill's network on December 19, 2023. After a comprehensive forensic investigation and extensive document review, North Hill was able to determine that certain data, including personal information, from the affected systems may have been accessed or acquired by the unauthorized party.

What Information Was Involved
Our forensic investigation is unable to conclude what specific information may have been accessed or acquired by the unauthorized party, so we are notifying you in the spirit of transparency. The information potentially involved may include your (or that of your relative, if you are receiving this letter as the next of kin of one of our former residents)

What We Are Doing
North Hill has taken a number of steps to ensure that our systems are secure. North Hill notified law enforcement of this incident and worked with security experts to enact additional security measures designed to stop a similar occurrence in the future. North Hill also is implementing additional security detection and response software.

What You Can Do
North Hill encourages you to take immediate steps to safeguard your personal information. Check your mail, email, phone calls, bank accounts, and health insurance statements for any suspicious activity. North Hill will cover the cost of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services. These services provide you with alerts for
from the date of enrollment when changes occur to your credit file.

This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. **To take advantage of this offer, please see the attached instructions**.

Please note that you can obtain information on fraud alerts from the following sources:

- Experian: (888) 397-3742; https://www.experian.com/fraud/center.html; National Consumer Assistance, P.O. Box 9554, Allen, TX 75013
- TransUnion: (800) 680-7289; https://www.transunion.com/fraud-alerts; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016-2000
- Equifax: (800) 525-6285; https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/. Fraud Victim Assistance Department, Consumer Fraud Division, P.O. Box 105788, Atlanta, GA 30348-5788

If you think that your personal information is being improperly used, you can also contact local law enforcement to file a police report. Finally, you can contact the Federal Trade Commission ("FTC") at 1-877-ID THEFT (877-438-4338), via mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580, or review the information on identity theft promulgated by the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/.

For More Information
If you have any questions or concerns, please do not hesitate to contact our dedicated call center at 1-833-919-4779. The call center is available Monday – Friday 8:00 am – 8:00 pm Eastern time, excluding holidays. North Hill understands the importance of safeguarding your personal information and takes that responsibility very seriously. We will do all we can to assist any individuals whose personal information may have been compromised and help them work through the process.

Thank you,

Joseph A. Frias
President and Chief Executive Officer
North Hill Communities, Inc.

Additional Information

How do I enroll for the free services?

To enroll in credit monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/nhci** and follow the instructions provided. When prompted please provide the following unique code to receive services: . In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (18) years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Security Freeze

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three (3) major consumer reporting agencies: Equifax, Experian and TransUnion. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail to the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

- Experian Security Freeze: (888) 397-3742; https://www.experian.com/freeze/center.html; P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze: (888) 909-8872; https://www.transunion.com/credit-freeze; P.O. Box 160, Woodlyn, PA 19094
- Equifax Security Freeze: (800) 349-9960; https://www.equifax.com/personal/credit-report-services/credit-freeze/; P.O. Box 105788, Atlanta, GA 30348

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived during the prior five (5) years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report.

You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

State-Specific Information

For Massachusetts residents: Under Massachusetts law, individuals have the right to obtain any police report filed in regard to this event.

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 56 Rhode Island residents impacted by this incident.

For New York residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

For North Carolina residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

North Hill Communities Inc.
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08461 1-1

To the Estate of
[redacted]

February 14, 2024

Dear Estate of [redacted],

On behalf of North Hill Communities, Inc., North Hill Home Health Care, Inc., North Hill Needham, Inc., Connected for Life, Inc., and the North Hill Employee Dental Plan (collectively, "North Hill"), we are sending this letter to you as part of our commitment to the privacy of our community. We take the security of our current and former residents, employees and dental plan participants very seriously.

What Happened
On December 26, 2023, North Hill detected a cybersecurity incident affecting certain systems in our network environment. North Hill immediately secured the network and engaged third party information technology and forensic specialists to assist with restoring systems and investigating the extent of the unauthorized activity. The forensic investigation revealed that an unauthorized party gained access to North Hill's network on December 19, 2023. After a comprehensive forensic investigation and extensive document review, North Hill was able to determine that certain data, including personal information, from the affected systems may have been accessed or acquired by the unauthorized party.

What Information Was Involved
Our forensic investigation is unable to conclude what specific information may have been accessed or acquired by the unauthorized party, so we are notifying you in the spirit of transparency. The information potentially involved may include your relative's

What We Are Doing
North Hill has taken a number of steps to ensure that our systems are secure. North Hill notified law enforcement of this incident and worked with security experts to enact additional security measures designed to stop a similar occurrence in the future. North Hill also is implementing additional security detection and response software.

What You Can Do
North Hill encourages you to take immediate steps to safeguard your relative's personal information. Check any mail, email, phone calls, bank accounts and health insurance statements for any suspicious activity.

Please note that you can obtain information on fraud alerts from the following sources:

- Experian: (888) 397-3742; https://www.experian.com/fraud/center.html; National Consumer Assistance, P.O. Box 9554, Allen, TX 75013

- TransUnion: (800) 680-7289; https://www.transunion.com/fraud-alerts; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016-2000
- Equifax: (800) 525-6285; https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/. Fraud Victim Assistance Department, Consumer Fraud Division, P.O. Box 105788, Atlanta, GA 30348-5788

If you think that your relative's personal information is being improperly used, you can also contact local law enforcement to file a police report. Finally, you can contact the Federal Trade Commission ("FTC") at 1-877-ID THEFT (877-438-4338), via mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580, or review the information on identity theft promulgated by the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/.

For More Information
If you have any questions or concerns, please do not hesitate to contact our dedicated call center at 1-833-919-4779. The call center is available Monday – Friday 8:00 am – 8:00 pm Eastern time, excluding holidays. North Hill understands the importance of safeguarding personal information and takes that responsibility very seriously. We will do all we can to assist any individuals whose personal information may have been compromised and help them work through the process.

Thank you,

Joseph A. Frias
President and Chief Executive Officer
North Hill Communities, Inc.

Additional Information

1. Notification of Death

The following steps are recommended for all deaths, regardless of age. It is best to notify all entities by telephone but such notifications **must** be followed-up in writing. Mail all correspondence certified, return receipt requested. Keep photocopies of all correspondence, including letters that you send.

1) Obtain at least twelve (12) copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
2) Immediately contact the credit reporting agencies (CRAs) in writing and request a "deceased" alert be placed on their credit report. You should also request a copy of the credit report.

3) Contact all credit issuers, collection agencies, the CRAs and any other financial institutions that need to know of the death using the required procedures for each one. Include the following information on all letters:
   - Name and SSN of deceased
   - Last known address
   - Last five (5) years of addresses
   - Date of birth
   - Date of death
   - To speed up processing, include all requested documentation specific to that agency in the first letter.
   - Send all mail certified, return receipt requested.
   - Keep copies of all correspondence, noting date sent and any response(s) you receive.
   - Contact each of the CRAs. Request a copy of the decedent's credit report. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
   - Request that the report is flagged with the following alert: "*Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship).*"
   - Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by case basis.

2. Specific Instructions from the 3 Credit Reporting Agencies

A. Experian

P.O. Box 9701
Allen, TX 75013

Ordering reports

- A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone and Internet. The spouse is legally entitled to the report.
- The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.

Requesting changes or voicing concerns

- A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request.
- After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor.
- If ID Theft is a stated concern, Experian will add a security alert after the file has been changed to

reflect the person as deceased.

- If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."

B. Equifax
P.O. Box 105139
Atlanta, GA 30348

To order a credit report
Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's' file. The request should include the following: A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)

For requests or changes
Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above.

Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven (7) year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.

C. TransUnion (TU)
P.O. Box 2000
Chester, PA 19016

Ordering reports

- TU requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file.
- If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TU will mail a credit file to the surviving spouse.
- If the deceased is a minor child of the requestor, TU will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.

Requesting changes or voicing concerns

- Placing a "decease alert" on reports: TU will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so.
- The requestor's phone number is added to the temporary, three (3) month alert. Upon receipt of a verifiable death certificate, TU will entirely suppress the decedent's credit file and so note it as a deceased consumer.
- TU will not mail out a copy of its contents without the requirements mentioned above.

If you suspect fraud, TU suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to **fvad@transunion.com**.

3. Addressing Suspected Fraud

In the event the estate suspected that the decedent's information has been misused, the estate can take the following steps:

- Request a copy of the decedent's credit report as outlined above.
- Place a "deceased alert" on the report as outlined above.
- Notify the police in the decedent's jurisdiction if you have evidence of fraud (collection notice, bills, credit report). A suspicion (especially of identity theft by a family member) is best when backed with concrete evidence.

- Notify any creditor, collection agency, credit issuer, utility company that the person is deceased and date of death. Be sure to include a copy of the death certificate. Request an immediate investigation and that they contact you with the results of the investigation. Insist on letters of clearance, which you should keep with the other estate papers.

In the event that the thief is a family member or relative, if the family is unable to decide on a course of action, it may be best to seek the advice of an attorney that specializes in estate or family law.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

State-Specific Information

For Massachusetts residents: Under Massachusetts law, individuals have the right to obtain any police report filed in regard to this event.

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 56 Rhode Island residents impacted by this incident.

For New York residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

For North Carolina residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

North Hill Communities Inc.
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08461 1-1

To the Parent or Guardian of
[redacted]

February 14, 2024

Dear Parent or Guardian of [redacted],

On behalf of North Hill Communities, Inc., North Hill Home Health Care, Inc., North Hill Needham, Inc., Connected for Life, Inc., and the North Hill Employee Dental Plan (collectively, "North Hill"), we are sending this letter to you as part of our commitment to the privacy of our community. We take the security of our residents, employees and dental plan participants very seriously.

On December 26, 2023, North Hill detected a cybersecurity incident affecting its network. North Hill has since remediated the issue and has taken a number of steps to ensure that our systems are secure. North Hill notified law enforcement of this incident and worked with security experts to enact additional security measures designed to stop a similar occurrence in the future. North Hill also is implementing additional security detection and response software.

North Hill encourages you to take immediate steps to safeguard your dependent's personal information. Check any mail, email, phone calls, bank accounts and health insurance statements for any suspicious activity. North Hill will cover the cost of Cyber Monitoring services for you and your minor child tw Cyber monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. To take advantage of this offer, please see the attached instructions.

Please note that you can obtain information on fraud alerts from the following sources:

- Experian: (888) 397-3742; https://www.experian.com/fraud/center.html; National Consumer Assistance, P.O. Box 9554, Allen, TX 75013
- TransUnion: (800) 680-7289; https://www.transunion.com/fraud-alerts; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016-2000
- Equifax: (800) 525-6285; https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/. Fraud Victim Assistance Department, Consumer Fraud Division, P.O. Box 105788, Atlanta, GA 30348-5788

If you think that your dependent's personal information is being improperly used, you can also contact local law enforcement to file a police report. Finally, you can contact the Federal Trade Commission ("FTC") at 1-877-ID THEFT (877-438-4338), via mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580, or review the information on identity theft promulgated by the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/.

If you have any questions or concerns, please do not hesitate to contact our dedicated call center at 1-833-919-4779. The call center is available Monday – Friday 8:00 am – 8:00 pm Eastern time, excluding holidays. North Hill understands the importance of safeguarding your dependent's personal information and takes that responsibility very seriously. We will do all we can to assist any individuals whose personal information may have been compromised and help them work through the process.

Thank you,

Joseph A. Frias
President and Chief Executive Officer
North Hill Communities, Inc.

Additional Information

How do I enroll for the free services?

To enroll in Cyber Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/nhci and follow the instructions provided. When prompted please provide the following unique code to receive services: . Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Security Freeze

You may also place a security freeze on your dependent's credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from your dependent's credit report without your written authorization. However, please be aware that placing a security freeze on your dependent's credit report may delay, interfere with, or prevent the timely approval of any requests your dependent make for new loans, credit mortgages, employment, housing or other services. Under federal law, your dependent cannot be charged to place, lift, or remove a security freeze.

You must place your dependent's request for a freeze with each of the three (3) major consumer reporting agencies: Equifax, Experian and TransUnion. To place a security freeze on your dependent's credit report, you may send a written request by regular, certified or overnight mail to the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

- Experian Security Freeze: (888) 397-3742; https://www.experian.com/freeze/center.html; P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze: (888) 909-8872; https://www.transunion.com/credit-freeze; P.O. Box 160, Woodlyn, PA 19094
- Equifax Security Freeze: (800) 349-9960; https://www.equifax.com/personal/credit-report-services/credit-freeze/; P.O. Box 105788, Atlanta, GA 30348

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your dependent's full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If your dependent has moved in the past five (5) years, the addresses where your dependent has lived during the prior five (5) years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security card, pay stub, or W2;
8. If your dependent is a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your dependent's credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you or your dependent to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you or your dependent will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and Social Security number) and the PIN number or password provided to you when you placed the security

freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

State-Specific Information

For Massachusetts residents: Under Massachusetts law, individuals have the right to obtain any police report filed in regard to this event.