

Attorney General Gordan MacDonald
Office of the Attorney General
33 Capitol Street
Concord NH 03301

2018 SEP -4 P 2: 10

Dear Attorney General MacDonald:

We are writing to notify you of a breach of security and unauthorized access or use of personal information involving NH residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

We recently became aware of a situation where an unauthorized party accessed one of our employee's email accounts. We discovered this situation on August 15, 2018 and took immediate steps to shut down access to the account. We promptly engaged our IT support to help us investigate, evaluate and respond to the situation. Based on their review of the situation and an examination of the impacted email account, it is possible that some personal data belonging to our employees and our subcontractors' employees was potentially exposed to the unauthorized intruder. This data may have included personally identifiable information (PII) with some combination of your name, address, social security number and mother's-maiden-name.

NUMBER OF NH RESIDENTS AFFECTED

There were six individuals that were affected in NH whose personal information was subject of this incident. The NH residents have received or will shortly receive notice by mail. We have included a copy of the notice that will be sent to all affected NH residents.

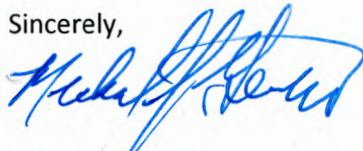
STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

We take our responsibilities to protect our customer's and employee information *very* seriously. We have contracted with Cyberscout to notify all persons who may be affected by this data breach. We are offering 12 months of Triple Bureau Credit Monitoring and Triple Bureau Credit Reports. We have trained employees on additional safety measures. And we are in the process of setting up 2 factor authentications for all e-mail accounts.

CONTACT INFORMATION

Please contact Michael Gervino, President of Mechanical Construction & Services Inc. 603-681-1900 if you have any questions or need further information.

Sincerely,



Michael J. Gervino
President

Sample letter to be
sent to NHI
Residents

Date

Name

Address

Address

Address

Dear:

Please read this letter in its entirety.

We recently became aware of a situation where an unauthorized party accessed one of our employee's email accounts. We discovered this situation on xx x, 2018, and took immediate steps to shut down access to the account. We promptly engaged our IT support to help us investigate, evaluate and respond to the situation. Based on their review of the situation and an examination of the impacted email account, it is possible that some personal data belonging to you was potentially exposed to the unauthorized intruder. This data may have included personally identifiable information (PII) with some combination of your name, address, social security number and mother's-maiden-name.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What is <OUR COMPANY> doing to address this situation?

<OUR COMPANY> has made immediate enhancements to our systems, security and practices to ensure that appropriate security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation. That's why <OUR COMPANY> is providing you with access to **Triple Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have. These services will be provided by **CyberScout** a company that specializes in identity theft education and resolution.

How do I enroll for the free services?

To enroll in **Credit Monitoring*** services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. **When prompted please provide the following unique code to receive services: <CODE HERE.>**

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with your unique code.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 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.

What can I do on my own to address this situation?

CyberScout has been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts. However, if you choose not to use these services, we are strongly urging all employees to consider the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to <OUR COMPANY> or CyberScout

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

What if I want to speak with OUR COMPANY regarding this incident?

While CyberScout should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with [COMPANY NAME] regarding this incident. If so, please call XX at XXX-XXX-XXXX from (enter times) Eastern Time, Monday through Friday.

At <OUR COMPANY> we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

JANE DOE
President and CEO