gravel & shea | ATTORNEYS AT LAW

A PROFESSIONAL CORPORATION

76 St. Paul Street
P.O. Box 369
Burlington, Vermont 05402-0369

Telephone 802.658.0220
Facsimile 802.658.1456
www.gravelshea.com

Heather Rider Hammond
Shareholder
hhammond@gravelshea.com

April 9, 2018

New Hampshire Department of Justice
Attn: Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Security Incident

Dear Attorney General MacDonald:

This firm represents Control Technologies, Inc. ("CTI") with respect to an incident involving the potential exposure of certain personal information described in detail below.

1. Nature of the security breach or unauthorized use or access.

On or about April 4, 2018, CTI became aware that it had been affected by a breach on February 22, 2018. It realized that it had been subject to an email attack when forged emails were being sent to a CTI employee's email accounts from someone appearing to be a company executive. CTI immediately contacted its IT Manager who blocked the emails, and it has contacted the authorities. It also began running deep scans and reviewing its systems to identify potential network issues and their source. Through the programmatic and manual review of an employee email account, the company determined that the information related to some employees and included their names, addresses, Social Security numbers and earnings information that was contained in the email account at the time it was accessed by the unknown individual(s).

2. Number of New Hampshire residents potentially affected.

Approximately 89 New Hampshire residents have potentially been affected. The company sent the impacted residents individual letters via email notifying them of the incident on April 9, 2018. A copy of the notice is attached to this letter, which informs these individuals about the 12 months of credit reporting and identity theft protection services that are being offered to them.

3. Steps taken or plan to take relating to the potential incident.

CTI has taken steps to secure employee information, including reviewing and revising policies and procedures, enhancing the security protocols on their servers and introducing encryption protocol to protect email content. It has also advised state and federal taxing authorities and law enforcement.

4. Other notification and contact information.

If you have additional questions, please contact me at hhammond@gravelshea.com or (802) 658-0220.

Very truly yours,

GRAVEL & SHEA PC

Heather Rider Hammond

HRH:snc

Enclosure

CONTROL TECHNOLOGIES
DEFINING BUILDING PERFORMANCE

April 9, 2018

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

NOTICE OF DATA BREACH

We are writing to notify you that the unauthorized acquisition of your personal information may have occurred on February 22, 2018. You are receiving this letter because you are an employee or a former employee of Control Technologies.

What Happened?

On April 4, 2018, we discovered that our company was affected by a breach on February 22, 2018. We have immediately contacted the authorities. We also began running deep scans and reviewing our systems to identify potential issues of our network and its source.

What Information Was Involved?

We determined that the information related to some of you included your full name, address, Social Security number and earnings information that may have been compromised by an unknown individual(s).

What We Are Doing.

We take the security of your information very seriously. In addition to the steps outlined above, we have notified the FBI and the credit agencies. We have been working to ensure the security of our systems and confirm the nature and scope of this incident. We are committed to continuing employee training designed to help identify and properly report potential email phishing scams. Lastly, we are providing notice of this event to the state Attorneys General and other state agencies as required and we will work with law enforcement in any criminal investigation.

As an added precaution, to help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: July 31, 2018 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL
- Provide your **activation code**: [**code**]

What You Can Do.

We encourage you to take advantage of the complimentary identity theft and fraud service offered above. Additionally, we strongly recommend that you remain vigilant by monitoring your accounts and reporting any suspected identity theft to credit law enforcement. You should consider taking the following steps to protect yourself:

1. Review your bank, credit card and debit card account statements over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.

2. Monitor your credit reports with the major credit reporting agencies.

Equifax	*Experian*	*TransUnion*
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

By law, you are entitled to a free copy of your credit report from those agencies every twelve months. Call the credit reporting agency at the telephone number on the report if you find:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address and Social Security number.

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and file a report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

4. If you find suspicious activity on your credit reports or on your other account statements, consider placing a fraud alert on your credit files, so creditors will contact you before opening new accounts. You may also place a credit freeze on your credit files, which will new accounts from being opened under your name without a special PIN. Be aware that a credit freeze will also prevent potential creditors from accessing your credit report unless you temporarily lift the freeze, so it may delay your ability to obtain credit. Please call the three credit reporting agencies at the number or website address below to place a fraud alert or credit freeze.

Equifax:	888-766-0008 or https://www.freeze.equifax.com/
Experian:	888-397-3742 or http://www.experian.com/consumer/security_freeze.html
TransUnion:	800-680-7289 or https://freeze.transunion.com/

To request a credit freeze, you will need to provide your full name, social security number, date of birth, addresses over the last five years, proof of current address and a copy of your government -issued identification. Each credit agency may charge up to $10 for a credit freeze, unless you can show that you were a victim of identity theft by provide a copy of the police report, investigative report, or complaint to law enforcement agency regarding the theft.

For More Information.

In our decades of business, this is our first direct encounter with cyber-crime. Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have any questions, contact Human Resources at 802-764-2200, or at hr@controltechinc.com.

We sincerely regret any inconvenience or concern this may have caused.

Sincerely,

Len Pattison	F. Bruce Merges
President	CEO