MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 30, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Incident

Dear Attorney General MacDonald:

We represent Rosenberg & Manente, PLLC ("Rosenberg & Manente") 12 W. 32nd Street, 10th Floor, New York, NY 10001, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. By providing this notice, Rosenberg & Manente does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statutes, or personal jurisdiction.

Background

On June 11, 2018 Rosenberg & Manente, PLLC ("Rosenberg & Manente") became aware of suspicious activity regarding employees' email accounts. Rosenberg & Manente immediately began an investigation to confirm the security of their network and to determine the nature and scope of this event. With the assistance of third party forensic investigators, Rosenberg & Manente learned that unknown and unauthorized individuals accessed certain employee email accounts between June 5, 2018 and June 11, 2018. Rosenberg & Manente engaged third-party forensic investigators to review each email message body and each document from the affected email accounts determined to be accessed by the unauthorized actor, to identify whether any sensitive information pertaining to individuals or business entities was exposed. In September 2018, Rosenberg & Manente confirmed the types of information relating to certain individuals and entities that may have been viewed by the unauthorized actor. Once they confirmed the information and individuals who were potentially impacted by this incident, Rosenberg & Manente began diligently working to identify addresses and affiliations for affected individuals. This was a thorough process to ensure an accurate notice was provided to all potentially affected individuals.

Notice to New Hampshire Resident

Rosenberg & Manente provided written notice to potentially affected individuals, which includes one (1) New Hampshire resident, by mail, on or about November 30, 2018. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Rosenberg & Manente is providing all potentially affected individuals complimentary access to 12 free months of credit and identity monitoring services, including identity restoration services, through Transunion. Additionally, Rosenberg & Manente is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rosenberg & Manente is also providing written notice of this incident to other state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EXHIBIT A

ROSENBERG&MANENTE, PLLC
Certified Public Accountants

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Rosenberg & Manente, PLLC ("Rosenberg & Manente") is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so.

What Happened? On June 11, 2018 Rosenberg & Manente became aware of suspicious activity regarding employees' email accounts. We immediately began an investigation to confirm the security of our network and to determine the nature and scope of this event. With the assistance of third party forensic investigators, we learned that unknown and unauthorized individuals accessed certain employee email accounts between June 5, 2018 and June 11, 2018. Rosenberg & Manente engaged third-party forensic investigators to review each email message body and each document from the affected email accounts determined to be accessed by the unauthorized actor, to identify whether any sensitive information pertaining to individuals or business entities was exposed. In September 2018, Rosenberg & Manente confirmed the types of information relating to certain individuals and entities that may have been viewed by the unauthorized actor. Once they confirmed the information and individuals who were potentially impacted by this incident, Rosenberg & Manente began diligently working to identify addresses and affiliations for affected individuals. This was a thorough process to ensure an accurate notice was provided to all potentially affected individuals.

What Information Was Involved? Since this incident was discovered, Rosenberg & Manente has received no indication that any personal information in the email accounts has been misused by an unauthorized party. However, we are providing notice to you out of an abundance of caution. Our investigation determined the following types of information were stored within an impacted email account and may have been subject to unauthorized access or acquisition: name and **<<data elements>>**.

What We Are Doing. Rosenberg & Manente is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed the log-in credentials for all employee email accounts to prevent further unauthorized access. Since then, we have continued ongoing efforts to enhance security controls and to implement additional controls, including use of multi-factor authentications to help protect employee email accounts from unauthorized access.

As an added precaution, we are offering you access to <<credit monitoring months>> of free credit/identity monitoring and identity restoration services through TransUnion. We encourage you to take advantage of these identity protection services. To enroll in these services, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode **<<Insert static six-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain <<credit monitoring months>> of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

What You Can Do. You can review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud.* You can also enroll to receive the free services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. Please call 1-855-288-5422, Monday through Friday, 8:00 a.m. to 6:00 p.m. E.S.T (excluding U.S. holidays).

We sincerely regret the inconvenience this incident causes for you. Rosenberg & Manente remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Philip Rosenberg

Philip Rosenberg, CPA
Managing Partner
Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.