MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

December 18, 2020

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Devine, Millimet & Branch, P.A. ("Devine") located at 111 Amherst Street Manchester, NH 03101, and write to notify your office of an incident that may affect the security of some personal information relating to twelve thousand eight hundred and forty-six (12,846) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Devine does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 24, 2020, Devine became aware that Devine discovered files were encrypted by ransomware. Devine immediately began an investigation to determine the full nature and scope of the event and what, if any, data was impacted. The investigation determined that files located on the impacted systems were accessed and acquired by an unauthorized actor. However, the specific files on the impacted system that were taken could not be determined. On October 20, 2020, Devine determined that certain client and employee information was located on the impacted servers where data could have been removed. In an abundance of caution, notice was provided to individuals whose personal information was contained on the impacted systems, including clients and employees.

The information that could have been subject to unauthorized access includes name, address, Social Security number, date of birth, and/or account numbers.

Notice to New Hampshire Residents

On December 18, 2020, Devine provided written notice of this incident to all affected individuals, which includes twelve thousand eight hundred and forty-six (12,846) New Hampshire residents. Written notice is being provided in substantially the same form as the letters attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Devine moved quickly to investigate and respond to the incident, assess the security of Devine systems, and notify potentially affected individuals. Devine is also working to implement additional safeguards and training to its employees. Devine is providing access to credit monitoring services for twenty-four (24) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/smm

EXHIBIT A

DEVINE MILLIMET

ATTORNEYS AT LAW

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: Cybersecurity Breach Notification

Dear <<Name 1>>:

Over the past several years, Devine Millimet has spent hundreds of thousands of dollars on updated equipment, software and an outside security contractor to address the ever-increasing threat of cybercrime. Unfortunately, in spite of our efforts, we have recently become aware of a cyberattack that affected a portion of our Firm's information technology ("IT") system. We take the security of our employees' information very seriously and want to let you know what we have learned about this attack.

What Happened

On August 24, 2020, Devine Millimet became aware of a ransomware encryption attack that affected multiple servers in our IT system. Our security contractor identified the ongoing attack, stopped it, and immediately began restoration of the affected servers from stored backups and our normal operations resumed. However, within a few days of the restoration, we received communication from the cybercriminals alleging that they had successfully copied and removed some data from our system. On October 20, 2020, we determined that certain employee information was located on the impacted servers where data could have been removed. While we are unable to confirm (1) whether your information was stored on one of the impacted servers and (2) if so, whether your information was among the stolen information, we are notifying you as your information may have been stored on the impacted systems.

What Devine Millimet Is Doing

Upon receipt of the communication from the cybercriminals, we immediately retained a third party forensic consultant to investigate the attack. We subsequently reported the attack to the Federal Bureau of Investigation Cyber Crimes Unit and their investigation is ongoing.

Working with our own security contractor and the forensic consultant, Devine installed additional security software to enhance the threat protection that was already in place at the time of the attack. In addition, through our forensic consultant, we took what we believe to be the necessary steps to prevent the distribution of any data that may have been removed during the attack. At this time, we have no reason to believe that any data went beyond the control of the cybercriminals, nor do we have any reason to believe that any data was, or will be, misused or publicly disseminated.

As an added precaution, we are also offering you complimentary access to twenty-four (24) months of credit monitoring and identity theft restoration services through TransUnion. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Information Was Involved

Based on the available evidence, we determined that the cybercriminal accessed our environment beginning on August 13, 2020. Due to the sophistication of the attack, our forensic consultant was unable to determine what data may have actually been removed by the cybercriminals. We do know that the cybercriminal did not have access to any credit card account numbers, as that information is not retained anywhere in our system. However, based on the work

of our forensic consultant, we understand that the criminals accessed our network and potentially stole data from a document management server that contained archived client/matter information, a portion of an email server, and an administrative file server. Depending on what information you may have previously provided to us in connection with your employment, it is possible that social security numbers, dates of birth and/or account numbers could be included in the data stored on those servers.

While we are unable to confirm (1) whether any of your information was stored on one of the impacted servers and (2) if so, whether your information was included within the stolen files, we are notifying you of this incident, as your information may have been stored on the impacted systems.

For More Information

We truly value your relationship with Devine Millimet and sincerely regret any inconvenience that this criminal cyberattack may cause you. Should you have any further questions or concerns regarding this incident, please contact our dedicated assistance line at 800-269-0636, Monday through Friday, from 9am to 9pm EST.

Very truly yours,

Devine, Millimet & Branch,
Professional Association

Charles T. Giacopelli, Esq.
President

Steps You Can Take to Help Protect Your Information

Enroll in Credit and Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity 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 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.

Monitor Accounts

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 **P.O. Box 9554** **Allen, TX 75013** **1-888-397-3742** **www.experian.com/freeze/center.html**	**TransUnion** **P.O. Box 160** **Woodlyn, PA 19094** **1-888-909-8872** **www.transunion.com/credit-freeze**	**Equifax** **P.O. Box 105788** **Atlanta, GA 30348-5788** **1-800-685-1111** **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.); and
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 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	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

Additional 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 86 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, 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.)

DEVINE MILLIMET

ATTORNEYS AT LAW

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: Cybersecurity Breach Notification

Dear <<Name 1>>:

Over the past several years, Devine Millimet has spent hundreds of thousands of dollars on updated equipment, software and an outside security contractor to address the ever-increasing threat of cybercrime. Unfortunately, in spite of our efforts, we have recently become aware of a cyberattack that affected a portion of our Firm's information technology ("IT") system. We take the security of our clients' information very seriously and want to let you know what we have learned about this attack.

What Happened

On August 24, 2020, Devine Millimet became aware of a ransomware encryption attack that affected multiple servers in our IT system. Our security contractor identified the ongoing attack, stopped it, and immediately began restoration of the affected servers from stored backups and our normal operations resumed. However, within a few days of the restoration, we received communication from the cybercriminals alleging that they had successfully copied and removed some data from our system.

What Devine Millimet Is Doing

Upon receipt of the communication from the cybercriminals, we immediately retained a third party forensic consultant to investigate the attack. We subsequently reported the attack to the Federal Bureau of Investigation Cyber Crimes Unit and their investigation is ongoing.

Working with our own security contractor and the forensic consultant, Devine installed additional security software to enhance the threat protection that was already in place at the time of the attack. In addition, through our forensic consultant, we took what we believe to be the necessary steps to prevent the distribution of any data that may have been removed during the attack. At this time, we have no reason to believe that any data went beyond the control of the cybercriminals, nor do we have any reason to believe that any data was, or will be, misused or publicly disseminated.

As an added precaution, we are also offering you complimentary access to twenty-four (24) months of credit monitoring and identity theft restoration services through TransUnion. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Information Was Involved

Based on the available evidence, we determined that the cybercriminal accessed our environment beginning on August 13, 2020. Due to the sophistication of the attack, our forensic consultant was unable to determine what data may have actually been removed by the cybercriminals. We do know that the cybercriminal did not have access to any credit card account numbers, as that information is not retained anywhere in our system. However, based on the work of our forensic consultant, we understand that the criminals accessed our network and potentially stole data from a

document management server that contained archived client/matter information, a portion of an email server, and an administrative file server. Depending on what information you may have previously provided to us in connection with your matter, it is possible that social security numbers, dates of birth and/or account numbers could be included in the data stored on those servers.

While we are unable to confirm (1) whether any of your information was stored on one of the impacted servers and (2) if so, whether your information was included within the stolen files, we are notifying you of this incident, as your information may have been stored on the impacted systems.

For More Information

We truly value your relationship with Devine Millimet and sincerely regret any inconvenience that this criminal cyberattack may cause you. Should you have any further questions or concerns regarding this incident, please contact our dedicated assistance line at 800-269-0636, Monday through Friday, from 9am to 9pm EST.

Very truly yours,

Devine, Millimet & Branch,
Professional Association

Charles T. Giacopelli, Esq.
President

Steps You Can Take to Help Protect Your Information

Enroll in Credit and Identity Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity 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 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.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, 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.)