CARMODY
TORRANCE | SANDAK | HENNESSEY LLP

Sherwin M. Yoder
Partner
Main: 203-777-5501
Direct: 203-784-3107
Fax: 203-784-3199
syoder@carmodylaw.com

195 Church Street
P.O. Box 1950
New Haven, CT 06509-1950

January 22, 2021

Via E-Mail Only: attorneygeneral@doj.nh.gov

Gordon J. MacDonald
Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301

Re: Breach of Security Involving Computerized Data

Dear Attorney General MacDonald:

Pursuant to New Hampshire R.S.A. Section 359-C:20(l)(b), I write to notify your office that our client suffered a ransomware incident that may have resulted in the unauthorized disclosure of personal information of two (2) New Hampshire residents.

Background of Incident and Response

On October 5, 2020, TrustLawyer LLC's ("TrustLawyer") IT provider discovered that the firm had suffered a ransomware incident. Systems were restored from clean back-ups and there was never any contact or communications with any individual behind the ransomware attack. The ensuing forensic investigation uncovered that a system folder had been encrypted by the ransomware and that it contained personal information of certain estate clients and beneficiaries.

The Nature of the Potentially Compromised Data

The forensic examination was completed by December 24, 2020, and revealed that the personal information of 2 New Hampshire individuals was contained within the affected system folder. The types of information that may have been compromised during this unauthorized access include names and Social Security numbers.

There is no forensic evidence that the ransomware involved access to, or exfiltration of, personal data. Nevertheless, the forensic examination could not rule out the possibility that the subject files were accessed or downloaded.

What TrustLawyer Has Done and Is Doing

With the support of its IT provider, TrustLawyer has taken the following measures to prevent or mitigate future unauthorized access: (1) reset compromised passwords; (2) increased social engineering training for TrustLawyer staff; and (3) implemented tighter protocols for patching systems and for scanning for suspicious or malicious e-mail links and attachments.

TrustLawyer engaged undersigned breach counsel to provide, simultaneously with this Attorney General notification, individual letter notification to each of the potentially impacted individuals. TrustLawyer has also engaged CyberScout (https://cyberscout.com/en) to provide identity theft detection and resolution services for twenty-four (24) months for all affected Connecticut residents at no cost to them. An exemplar of the individual notification letters is enclosed.

Thank you for your consideration. If I may answer any questions or provide additional information, please contact me directly at (203) 784-3107 or syoder@carmodylaw.com.

Very truly yours,

Sherwin M. Yoder

SMY/ag
Encl.

TRUSTLAWYER, LLC

21 NEW BRITAIN AVENUE ROCKY HILL, CT 06067

PHONE: 860-257-4330 FAX 860-257-4388

JEFFREY L. CROWN
LAWYER

LISA HALLIGAN
ESTATE PARALEGAL

MARY PLATT
ADMINISTRATIVE ASSISTANT

Date

[NAME]
[STREET ADDRESS]
[CITY, CT, ZIP]

Re: Possible Compromise of Personal Information / Identity Theft Protection Services

To my valued clients their families:

Thank you for your trust and confidence. Because I respect the privacy of your information, as a precautionary measure I am writing to let you know about a data security incident that occurred recently.

What Happened?

On October 5, 2020, we suffered a ransomware incident that resulted in the compromise of our computer system. Immediately upon discovering the incident, our IT provider restored our systems to prevent further unauthorized access.

A forensic investigation followed and, as a result, the forensic investigator recently discovered that the incident may have resulted in the disclosure of some of your personal information.

What Information Was Involved?

Although we have not concluded that any individual has actually accessed your personal information, we cannot rule out that possibility. As a precautionary measure, we are notifying potentially affected individuals. The types of information that may have been compromised during this incident include your name, and Social Security number.

What Are We Doing?

Out of an abundance of caution, we are notifying you that the incident may have involved some of your personal information. We take the security and confidentiality of the personal information entrusted to us very seriously. We apologize for this situation and have taken the appropriate steps to ensure that sensitive information like this is appropriately secured against security incidents like this one.

We have taken and will continue to take action to prevent or mitigate future intrusions, including the engagement of a cybersecurity consultant to provide technical tools and staff training aimed at recognizing and avoiding suspicious and unexpected e-mails and downloads that may contain malicious software.

What Are We Doing to Protect Your Information?

We have made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation. In response to the incident, we are offering you services provided by CyberScout, a company specializing in fraud assistance and remediation services.

We are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score*** services at no charge. These services provide you with alerts for twenty four 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.

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.>** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud, as well as a $1,000,000 insurance reimbursement policy.

What additional information do you need and what steps can you take on your own?

Please read the enclosed "Information about Identity Theft Protection" section included with this letter. This section describes additional steps that you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

What if I want to speak with someone regarding this incident?

If you would like to discuss this incident further, please call me at 860-257-4330. from 9:00 to 4:00, Monday through Thursday.

We take our responsibilities to protect personal information very seriously and offer our sincerest apologies for any inconvenience this may cause.

Sincerely,

Jeffrey L. Crown

Encl.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Connecticut: You may also obtain information about preventing and avoiding identity theft from the Connecticut Office of Attorney General:

Connecticut Office of the Attorney General, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, https://portal.ct.gov/AG/Consumer-Issues/Identity-Theft/Identity-Theft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report, if any.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

The next 2 paragraphs are regarding incidents involving personal health information. Disregard if not applicable to your situation.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.