



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

JAN 04 2022

CONSUMER PROTECTION

Gregory Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E Main Street
Soundview Plaza
Suite 700R
Stamford, CT 06902

December 30, 2021

VIA U.S. MAIL

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

Re: Preliminary Notice of Data Security Event

Dear Sir or Madam:

We represent The Marker Group Inc. ("Marker Group") located at 13105 Northwest Freeway, Suite 300, Houston, Texas 77040, and are writing to provide your Office with preliminary notice of a recent data security event that may affect the security of personal information related to New Hampshire residents. By providing this preliminary notice, Marker Group does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction. This notice will be supplemented with any new, significant facts learned after its submission, including the total number of impacted New Hampshire residents.

Marker Group provides litigation support services to law firms in the United States, including hosting data for law firms' share and access during the course of a lawsuit. The information involved in this event is associated with third party lawsuits for which Marker Group provides litigation support services.

On September 3, 2021, Marker Group discovered suspicious activity on certain systems in its computer network. As a result, Marker Group immediately worked to secure its environment and, with the assistance of third-party computer specialists, launched an investigation to determine the nature and scope of the activity. On or about September 10, 2021, the investigation determined that certain files in Marker Group's systems may have been accessed by an unknown, unauthorized third party.

Marker Group therefore began a lengthy and time-intensive, thorough review of the potentially impacted folders and its internal files and systems in order to identify the information that was potentially impacted and to whom it related. Marker Group continues to diligently review the information and reconcile this information with its internal records in furtherance of identifying the individuals to whom the data relates and the appropriate contact information for those individuals. While the review is ongoing, at this time Marker Group has identified twelve (12) New Hampshire residents associated with protected information that may have been accessed by the actor.

Mullen.law

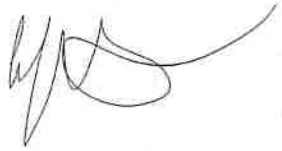
Office of the New Hampshire Attorney General
December 30, 2021
Page 2

On December 23, 2021, Marker Group notified all currently-identified individuals and will issue direct notice to additional individuals as they are discovered during the ongoing review. Importantly, there is no indication that individuals' specific information was or will be misused. However, Marker Group is notifying all potentially impacted individuals as quickly as possible out of an abundance of caution.

Marker Group will supplement this notice to your Office and provide the total number of impacted New Hampshire residents upon completion of its review and identification of all impacted individuals.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'GB', followed by a vertical line.

Gregory Bautista of
MULLEN COUGHLIN LLC

GJB:rrg
Enclosure

Exhibit A



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

<<MailID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Notice of Data <<Variable 1>>

The Marker Group is writing to make you aware of an incident that may affect the privacy of some of your information. Marker Group provides litigation support services to law firms in the United States, including hosting data for law firms to share and access during the course of a lawsuit. You are receiving this letter because you are associated with a litigation matter in which your personal information was involved. This letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? On September 3, 2021, Marker Group discovered suspicious activity on certain systems in our computer network. As a result, we immediately worked to secure our environment and, with the assistance of third-party computer specialists, launched an investigation to determine the nature and scope of the activity. On or about September 10, 2021, the investigation determined that certain files on our systems may have been accessed by an unknown, unauthorized third party. We immediately began a review of the potentially impacted files and our internal systems to identify the information involved and to whom it related. Unfortunately, on December 13, 2021, we determined that certain files containing your information could have been accessed during the event. While there is no indication that your specific information was or will be misused, we are notifying all potentially impacted individuals out of an abundance of caution.

What Information was Involved? Our investigation determined that the following types of information related to you may have been impacted: name, date of birth, Social Security number, and/or various types of medical records containing treatment and insurance information.

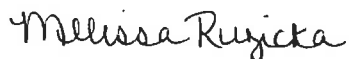
What we are Doing. We take this incident and the security of information in our care very seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our systems. We are reviewing our existing security policies and have implemented additional measures to further protect against similar incidents moving forward. We are notifying potentially impacted individuals, including you, so that you may take steps to protect your information.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<Insert 12 months or 24 months>> provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Individuals who wish to receive these services must enroll by following the enrollment instructions in the enclosed “*Steps You Can Take to Help Protect Your Information.*”

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your Explanation of Benefits and free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information.*"

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 855-604-1716 Monday through Friday, between 9:00 AM and 9:00 PM Eastern time. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Melissa Ruzicka".

Melissa Marker Ruzicka
Vice President
The Marker Group

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following unique 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 following 6-digit telephone pass code <<Insert static 6-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.

Once you are enrolled, you will be able to obtain << Insert 12 months or 24 months >> of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. 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, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and <<Insert Date>>. 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 credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 approximately [0] Rhode Island residents impacted by this incident.

RI DEPT OF JUSTICE
JAN 4 2022 4:11:38