

September 16, 2021

CONSUMER
Ross M. Molina, Esq.
504.702.1726 (direct)
Ross.Molina@WilsonElser.com

Sent Via U.S. Mail

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, New Hampshire 03302

Re: Our Client : Rockingham Mutual Group
Matter : Data Security Incident on October 2, 2020
Wilson Elser File # : 16516.01173

Dear Attorney General McDonald:

We represent Rockingham Mutual Group (“RMG”), which is headquartered in Harrisonburg, Virginia. Our representation of RMG relates to a potential data security incident described in more detail below. RMG takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security incident, the number of New Hampshire residents being notified, what information has been compromised, and the steps that RMG is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

It appears that on or around October 2, 2020, RMG was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate RMG’s computer network. While there is no evidence that any data was misused by the threat actor, this incident may have resulted in the compromise of personal information that is located on RMG’s system. The potentially impacted data elements varied by individual, and included full name in connection with social security number, driver’s license, passport, health insurance information, and personal health information.

RMG, however, is not aware of any evidence that information has been misused. RMG has not received any reports of related identity theft since the date of the incident (October 2, 2020 to present).

650 Poydras Street, Suite 2200 • New Orleans, LA 70130 • p 504.702.1710 • f 504.702.1715

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

2. Number of New Hampshire Residents Affected

A total of eleven (11) residents of New Hampshire were potentially affected by this security incident. Notification letters to these individuals will be mailed on September 17, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon learning of this incident, RMG moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. RMG has reviewed, altered and enhanced its policies and procedures relating to the security of its e-mail systems and servers. RMG is collaborating with the FBI in response to this incident. RMG has offered free credit monitoring services to all potentially affected individuals.

4. Contact Information

RMG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Ross.Molina@WilsonElser.com or 504.702.1726.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP


Ross M. Molina

Copy: Robert Walker, Esq. (Wilson Elser LLP)
Michael E. Kar, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*



Return to IDX
 P.O Box 989728
 West Sacramento, CA 95798-9728

To Enroll, Please Call:
 1-833-992-4003
 Or visit:
<https://app.idx.us/account-creation/protect>
 Enrollment Code: <<XXXXXXXXXX>>

Via First-Class Mail

<<First Name>> <<Last Name>>
 <<Address1>>
 <<Address2>>
 <<City>>, <<State>> <<Zip>>

September 17, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

Rockingham Mutual Group, Inc. (“RMG”) is an insurance company headquartered in Harrisonburg, Virginia. We are writing in order to inform you of an incident that may have exposed your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On October 2, 2020, RMG detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate RMG’s computer network. We immediately took steps to investigate and determine the nature of the incident, as well as enhance our network security measures. A comprehensive investigation was also done to identify any instances of sensitive data compromise. After finding no specific instances of sensitive data misuse, RMG arranged for notification of all individuals whose information could have potentially been compromised during the incident.

Accordingly, this letter serves to notify you that although we have found no evidence that your information has been specifically accessed for misuse, it is possible that your following information could have been exposed during the incident: full name; <<Variable1>>. We maintained this information on our system as part of insurance files and claims handled by RMG.

As of this writing, RMG has not received any reports of related identity theft since the date of the incident (October 2, 2020 present).

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate our incident response, which included conducting an investigation with the assistance of third-party forensic specialists and confirming the security of our network environment. We have been working with law enforcement to respond to this incident. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We value the safety of your personal information and are therefore offering <<12/24>> months of credit monitoring and identity theft protection services through IDX, which include:

- Single Bureau Credit Monitoring - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.
- CyberScan - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like Social Security Numbers, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
- Identity Theft Insurance - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
- Fully-Managed Identify Recovery - IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free IDX services by calling 1-833-992-4003 or by going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 8 a.m. – 8 p.m. Central Time. Please note the deadline to enroll is December 17, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

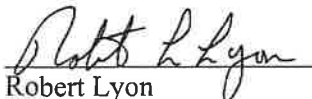
For More Information:

Enclosed hereto you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

Additionally, IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

RMG values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,


Robert Lyon
President & CEO

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed herein.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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. 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, 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 agencies 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 violators. 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 at 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.