



Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

November 13, 2024

Via Email: Idtheft@oag.state.md.us

Attorney General Anthony G. Brown

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Cybersecurity Incident
Client: RBN and Associates, Inc. d/b/a RBN Insurance Services

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents RBN and Associates, Inc. d/b/a RBN Insurance Services (“RBN”), an insurance broker specializing in the sale and management of property casualty and employee benefits plans located at 303 E. Wacker Drive, Suite 650, Chicago, Illinois 60601, with respect to a recent cybersecurity incident that was first discovered by RBN on May 15, 2024 (hereinafter, the “Incident”). RBN takes the security and privacy of the information within its control very 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 Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps RBN has taken to mitigate the Incident. We have also enclosed hereto a sample of the notification letter mailed to the potentially impacted individuals, which includes an offer for free credit monitoring services.

1. Nature of the Incident

On May 15, 2024, RBN detected unusual activity within an employee e-mail account. Upon discovery of this Incident, RBN immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. On June 11, 2024, the forensic investigation determined that the contents of one (1) RBN employee e-mail user account had been accessed and may have been acquired by an unauthorized actor. Evidence from the investigation indicated that unauthorized

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

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

wilsonelser.com

sign-ins first occurred on February 24, 2024, and unauthorized activity was discovered to have first occurred on March 5, 2024. No further unauthorized activity within RBN's e-mail environment was detected after May 15, 2024 and the impacted e-mail account has since been secured and remediated.

Based upon the findings of the forensic investigation, on July 10, 2024, RBN engaged a third-party data mining vendor to conduct a comprehensive review of the contents of the employee e-mail user account that was subject to unauthorized access for purposes of identifying those individuals whose personal information may have been impacted. The data mining review was completed on September 12, 2024. Although RBN is unaware of any fraudulent misuse of information, the data mining review determined that individuals' full names, addresses, dates of birth, payment card information, bank account information, medical information, life insurance information, health insurance information, and Social Security numbers may have been exposed as a result of the unauthorized activity. We note the impacted data elements vary per individual.

As of this writing, RBN has not received any reports of related identity theft since the date of the Incident (May 15, 2024, to present).

2. Number of Maryland residents affected.

Based upon the findings of the third-party data mining review, RBN identified fifty-two (52) residents of Maryland whose information was potentially impacted as a result of the Incident. Notification letters to these individuals will be mailed on November 14, 2024, via First Class Mail. A sample copy of the notification letter is attached hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

RBN is committed to ensuring the security and privacy of all personal information within its control and has taken steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, RBN moved quickly to investigate and respond to the Incident and assessed the security of its systems. Further, to prevent a similar incident from occurring in the future, RBN implemented the following security enhancements: performed a reset of all passwords across the organization, disabled web access to email, updated DMARC records, verified use of MFA (multi-factor authentication) across systems, reviewed data retention and data segmentation processes, and developed plans to upgrade active directory and to impose conditional access requirements.

Although RBN is not aware of any actual or attempted misuse of the affected personal information, RBN will be offering twelve (12) months of complimentary credit monitoring and identity theft restoration services to Maryland residents who were impacted by the incident to help protect their identity. Additionally, RBN will provide 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 the contact details for the Federal Trade Commission.

4. Contact information

RBN remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

EXHIBIT A

RBN & Associates, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November 14, 2024

VIA FIRST-CLASS MAIL

Notice of Data Incident

Dear [REDACTED],

RBN and Associates, Inc. d/b/a RBN Insurance Services ("RBN"), an insurance broker engaged in the sale and servicing of employee benefits plans, is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On May 15, 2024, RBN detected unusual activity within an employee e-mail account. Upon discovery of this incident, RBN immediately secured the account and promptly engaged a specialized third-party cybersecurity firm to conduct a comprehensive investigation to determine the nature and scope of the incident. The forensic investigation determined that one (1) RBN employee e-mail account may have been accessed by an unauthorized user. The e-mail account has since been secured and remediated.

Based on these findings, RBN engaged a third-party data mining firm to conduct a review of the information contained within the accessed e-mail account to identify the specific individuals and the types of information that may have been acquired by an unauthorized user. On September 12, 2024, RBN completed its review and finalized the list of individuals to notify.

What Information Was Involved?

As part of its business, RBN sells and services health insurance plans and other coverages for both employer groups and individual clients. RBN receives information from clients and prospective clients about individuals who are enrolled or eligible for coverage under their insurance plans. Your information may have been provided to RBN as an individual client, as a participant in a benefits plan purchased through RBN, or as someone potentially eligible for benefits purchased through RBN. Based on the investigation, the following information related to you may have been subject to unauthorized access: [REDACTED]

At this time, there is no evidence that any sensitive information has been misused by third parties as a result of this incident.

What We Are Doing

Data privacy and security is important to RBN, and it is committed to protecting the privacy and security of the personal information within its care. Since the discovery of the incident, RBN moved quickly to investigate, respond, and confirm the security of its systems. Further, to prevent a similar incident from occurring in the future, RBN conducts ongoing cybersecurity training for employees, updated DMARC records, verified use of multi-factor authentication across its systems, and will continue to take steps to mitigate the risk of future harm, including by updating its data retention and segmentation processes.

In response to the incident, RBN Insurance is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the unlikely event that you become subject to an incident of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of eighteen (18) years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse. We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have any questions or concerns not addressed in this letter, please call [REDACTED] (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Time (excluding U.S. national holidays).

RBN sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information within its control.

Sincerely,

RBN & Associates, Inc.

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed 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 for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.



00001020280000

P

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) 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 should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting <http://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at <https://dos.nysits.acsitefactory.com/consumerprotection>; by visiting the New York Attorney General at <https://ag.ny.gov> or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting <https://oag.dc.gov>, or emailing at consumer.protection@dc.gov.