MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

January 14, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus") located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079. We are writing to notify your office of an incident that may affect the security of some personal information relating to approximately four (4) residents.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information relates. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes name, address, passport number, medical information, and health insurance information.

Notice to Maryland Residents

On January 14, 2022, Rimkus began providing written notice of the event to affected individuals, which includes approximately four (4) resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT A

Rimkus Consulting Group, Inc.
12140 Wickchester Ln., Suite 300
Houston, Texas 77079

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: <<b2b_text_4(Notice of Data Event / Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Rimkus Consulting Group, Inc. ("Rimkus") is writing to notify you of a recent event that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? This past July, suspicious activity relating to three Rimkus employees' email accounts occurred. We quickly launched an investigation to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021, and issued emails to persons located within the Rimkus employees' email accounts. We promptly provided notice to each of the recipients of the erroneous emails.

We then worked with specialists to conduct a comprehensive review of information contained in the email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, we then conducted a manual review of our records to confirm the identities of individuals affected by this event and their contact information to provide notifications. On or around December 30, 2021, we completed our initial review as to your specific information.

Fortunately, the event was limited to only three employee email accounts, and the unknown actor did not obtain access to any other Rimkus accounts or systems.

What Information Was Involved? Our investigation determined that at the time of the event, your <<b2b_text_1(name, data elements)>> were stored within an impacted email account. To date, Rimkus has not received any reports of fraudulent misuse of anyone's information potentially impacted by this event.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event, and implement additional security measures to protect your information and our systems.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, we are offering you access to 24 months of complimentary credit monitoring services through Experian. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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 free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Protect Your Personal Information," which contains information on what you can do to safeguard against possible misuse of your information should feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services.

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at (855) 618-3185. This toll-free line is available Monday – Friday from 9:00 a.m. to 6:30 p.m. Eastern Time excluding U.S. holidays). You may also write to Rimkus at 12140 Wickchester Lane, Suite 300, Houston, TX 77079.

Sincerely,

John E. Orr
Senior VP, Marketing
Rimkus Consulting Group, Inc.

Steps You Can Take to Protect Your Personal Information

Enroll in Identity Theft Detection Services

To help protect your identity, we are offering a complimentary twenty-four (24) month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **<<b2b_text_6(activation deadline)>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<activation code s_n>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 890-9332 by **<<b2b_text_6(activation deadline)>>.** Be prepared to provide engagement number **<<b2b_text_5(engagement number)>>** as proof of eligibility for the identity restoration services by Experian.

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 one-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, 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

Additional Information

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 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 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 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 8 known Rhode Island residents impacted by this incident.

For Texas residents, you may report a security breach to the Texas Attorney General online at https://txoag.secure.force.com/CPDOnlineForm/. You may also reach the Texas Attorney General at: 300 W. 15th Street, Austin, Texas 78701, or by telephone at 1-800-252-8011, or by online form https://www.texasattorneygeneral.gov/contact-us-online-form.

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

February 15, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. Please accept this supplemental report as an update to our initial notification of January 14, 2022. A copy of the initial notification is attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

On January 19, 2022, Rimkus provided notice of this event to certain impacted owners of the data ("Data Owners") and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner, GEICO Insurance Company ("GEICO"), requested that Rimkus provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, and driver's license number.

Notice to Residents

On or about February 14, 2022, Rimkus began providing written notice of the event to affected individuals on behalf of GEICO, which includes approximately one (1) Maryland resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all our employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT A

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

January 14, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus") located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079. We are writing to notify your office of an incident that may affect the security of some personal information relating to approximately four (4) residents.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information relates. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes name, address, passport number, medical information, and health insurance information.

Notice to Maryland Residents

On January 14, 2022, Rimkus began providing written notice of the event to affected individuals, which includes approximately four (4) resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT B

Rimkus Consulting Group, Inc.
12140 Wickchester Lane, Suite
300 Houston, Texas 77079

[first_name] [middle_name] [last_name] [suffix]
[address_1]
[address_2]
[city], [state_province] [postal_code]

Re: Notice of Phishing Data Event

Dear [MemberFirstName] [MemberLastName]:

Rimkus Consulting Group, Inc. ("RCG"), a company which GEICO Insurance Company ("GEICO") does business with, is writing to notify you of a recent event that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? This past July, RCG noticed suspicious activity relating to certain RCG employees' email accounts. RCG quickly launched an investigation to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three RCG employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021, and issued emails to persons located within the RCG employees' email accounts. RCG promptly provided notice to each of the recipients of the erroneous emails.

RCG then worked with specialists to conduct a comprehensive review of information contained in the email accounts to determine what information was affected and to whom the information related. Upon completion of the third-party review, RCG then conducted a manual review of its records to confirm the identities of individuals affected by this event and their contact information to provide notifications. On or around December 30, 2021, RCG completed its initial review. Through the review, RCG determined that one of the email accounts contained information that was received from GEICO in the course of business operations and included your personal information. On January 19, 2022, RCG notified GEICO of the incident and that it had been determined that your personal information may have been included within the contents of the email account.

What Information Was Involved? RCG's investigation determined that at the time of the event, your name [Variable1] were stored within an impacted email account. To date, RCG has not received any indication that your data was viewed by another party and has not received reports of fraudulent misuse of anyone's information potentially impacted by this event.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event and to work with RCG in providing proper notifications.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, RCG is offering you access to two years of complimentary credit monitoring services through Experian. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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 free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Protect Your Personal Information," which contains information on what you can do to safeguard against possible misuse of your information should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services.

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at (855) 545-2581. This toll-free line is available Monday – Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to us at 12140 Wickchester Lane, Suite 300, Houston, TX 77079.

Sincerely,

John E. Orr
Senior VP, Marketing
Rimkus Consulting Group, Inc

Steps You Can Take to Protect Your Personal Information

Enroll in Identity Theft Protection Services

To help protect your identity, we are offering a complimentary twenty-four (24) month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: April 4, 2022 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [Variable2]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 288-8057 by April 4, 2022. Be prepared to provide engagement number # B023371 as proof of eligibility for the identity restoration services by Experian.

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 one-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, 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

Additional Information

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 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.

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

February 22, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("RCG"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of certain impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately four (4) Maryland residents. Please accept this supplemental report as an update to our initial notification of January 14, 2022 and our supplemental notification on February 15, 2022. A copy of the prior notifications are attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, RCG became aware of suspicious activity relating to certain employees' email accounts. RCG quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three RCG employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

RCG, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, RCG then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, RCG completed its review.

On January 14, 2022, RCG provided notice of this event to certain impacted owners of the data (“Data Owners”) and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner requested that RCG provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, driver’s license number, and medical information. Not all information was impacted for all residents.

Notice to Residents

On February 22, 2022, RCG began providing written notice of the event to affected individuals on the Data Owner’s behalf, which includes approximately four (4) Maryland residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, RCG immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

RCG is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, RCG is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. RCG also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. RCG is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, RCG does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT A

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

January 14, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus") located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079. We are writing to notify your office of an incident that may affect the security of some personal information relating to approximately four (4) residents.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information relates. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes name, address, passport number, medical information, and health insurance information.

Notice to Maryland Residents

On January 14, 2022, Rimkus began providing written notice of the event to affected individuals, which includes approximately four (4) resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

February 15, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. Please accept this supplemental report as an update to our initial notification of January 14, 2022. A copy of the initial notification is attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

On January 19, 2022, Rimkus provided notice of this event to certain impacted owners of the data ("Data Owners") and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner, GEICO Insurance Company ("GEICO"), requested that Rimkus provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, and driver's license number.

Notice to Residents

On or about February 14, 2022, Rimkus began providing written notice of the event to affected individuals on behalf of GEICO, which includes approximately one (1) Maryland resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all our employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT B

Rimkus Consulting Group, Inc.
12140 Wickchester Lane, Suite 300
Houston, Texas 77079

[First Name] [Last Name]
[Address #1]
[Address #2]
[City, State Zip Code]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[Date]

Dear [First Name] [Last Name]:

Rimkus Consulting Group, Inc. ("RCG") is writing to notify you of an event at RCG that may involve some of your information. RCG has your information because we provide engineering and consulting services for certain clients, including [Variable1]. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? This past July, RCG noticed suspicious activity relating to certain RCG employee email accounts. RCG quickly launched an investigation to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three RCG employee email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

RCG then worked with specialists to conduct a comprehensive review of information contained in the email accounts to determine what information was affected and to whom the information related. Upon completion of the third-party review, RCG conducted a manual review of its records to confirm the identities of individuals affected by this event and their contact information to provide notifications. Through the review, RCG determined that one of the email accounts contained information that was received from one or more of its clients in the normal course of business operations. On or around December 30, 2021, RCG completed its initial review. RCG notified its clients on or about January 14, 2022, and we are now notifying you.

What Information Was Involved? RCG's investigation determined that at the time of the event, your name and [Variable2] were stored within an impacted email account. To date, RCG has not received any reports of fraudulent misuse of anyone's information potentially impacted by this event.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event and to provide proper notifications.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, RCG is offering you access to two years of complimentary credit monitoring services through Experian. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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 free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Protect Personal Information," which contains information on what you can do to safeguard against possible misuse of your information should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services.

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at (855) 545-2581. This toll-free line is available Monday – Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to us at 12140 Wickchester Lane, Suite 300, Houston, TX 77079.

Sincerely,

John E. Orr
Senior VP, Marketing
Rimkus Consulting Group, Inc.

Steps You Can Take to Protect Personal Information

Enroll in Identity Theft Protection Services

To help protect your identity, we are offering a complimentary twenty-four (24) month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 4, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **[Variable3]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 288-8057 by April 4, 2022**.** Be prepared to provide engagement number **# B023371** as proof of eligibility for the identity restoration services by Experian.

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 one-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, 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

Additional Information

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 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 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/.

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

April 22, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately six (6) Maryland residents. Please accept this supplemental report as an update to our initial notification of January 14, 2022, our supplemental report on February 15, 2022, and our supplemental report on February 22, 2022. A copy of the the prior notifications are attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

On January 14, 2022, Rimkus provided notice of this event to certain impacted owners of the data ("Data Owners") and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner requested that Rimkus provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, driver's license number, medical information, and health insurance information.

Notice to Residents

On April 22, 2022, Rimkus began providing written notice of the event to affected individuals on the Data Owner's behalf, which includes approximately six (6) Maryland residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT A

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

January 14, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus") located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079. We are writing to notify your office of an incident that may affect the security of some personal information relating to approximately four (4) residents.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information relates. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes name, address, passport number, medical information, and health insurance information.

Notice to Maryland Residents

On January 14, 2022, Rimkus began providing written notice of the event to affected individuals, which includes approximately four (4) resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

February 15, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("Rimkus"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. Please accept this supplemental report as an update to our initial notification of January 14, 2022. A copy of the initial notification is attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, Rimkus became aware of suspicious activity relating to certain employees' email accounts. Rimkus quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

Rimkus, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its review.

On January 19, 2022, Rimkus provided notice of this event to certain impacted owners of the data ("Data Owners") and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner, GEICO Insurance Company ("GEICO"), requested that Rimkus provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, and driver's license number.

Notice to Residents

On or about February 14, 2022, Rimkus began providing written notice of the event to affected individuals on behalf of GEICO, which includes approximately one (1) Maryland resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, Rimkus immediately took steps to further secure its systems and investigate the event, increased phishing testing among all our employees, and implemented special phishing training for the three employees who were phished in the event.

Rimkus is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, Rimkus is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Rimkus also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Rimkus is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, Rimkus does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

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

February 22, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Rimkus Consulting Group, Inc. ("RCG"), located at 12140 Wickchester Lane, Suite 300, Houston, TX 77079, and are writing, on behalf of certain impacted data owner clients, to notify your office of an event that may affect the security of certain personal information relating to approximately four (4) Maryland residents. Please accept this supplemental report as an update to our initial notification of January 14, 2022 and our supplemental notification on February 15, 2022. A copy of the prior notifications are attached as ***Exhibit A*** for ease of reference.

Nature of the Data Event

This past July, RCG became aware of suspicious activity relating to certain employees' email accounts. RCG quickly launched an investigation, with third-party computer forensic specialists, to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three RCG employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

RCG, with the assistance of data review specialists, then initiated a comprehensive review of the information contained in the impacted email accounts to determine what information may have been affected and to whom the information related. Upon completion of the third-party review, RCG then conducted a manual review of its records to confirm the identities of individuals affected by the event and their contact information to provide notifications. On or around December 30, 2021, RCG completed its review.

On January 14, 2022, RCG provided notice of this event to certain impacted owners of the data ("Data Owners") and offered to fulfil disclosure obligations arising under U.S. data breach notice laws on behalf of the Data Owners. One such Data Owner requested that RCG provide notification directly to individuals and applicable regulators on its behalf.

Based on the review, the information that could have been subject to unauthorized access for Maryland residents includes: name, address, driver's license number, and medical information. Not all information was impacted for all residents.

Notice to Residents

On February 22, 2022, RCG began providing written notice of the event to affected individuals on the Data Owner's behalf, which includes approximately four (4) Maryland residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon learning of the event, RCG immediately took steps to further secure its systems and investigate the event, increased phishing testing among all its employees, and implemented special phishing training for the three employees who were phished in the event.

RCG is offering the affected individuals two years of complimentary credit monitoring and identity restoration services through Experian. Moreover, RCG is providing affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. RCG also is providing individuals with information on how to place a fraud alert and security freeze on a credit file, information on protecting against fraud, 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. RCG is also notifying other appropriate state regulators.

Conclusion

This notice may be supplemented if new significant facts are learned subsequent to its issuance. By providing this notice on behalf of impacted data owner clients, RCG does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the data event notification statute, or personal jurisdiction. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/tmr
Enclosure

EXHIBIT B

Rimkus Consulting Group, Inc.
12140 Wickchester Lane, Suite 300
Houston, Texas 77079

[first_name] [middle_name] [last_name] [suffix]
[address_1]
[address_2]
[city], [state_province] [postal_code]

April 22, 2022

[**Variable1**]

Dear [MemberFirstName] [MemberLastName]:

Rimkus Consulting Group, Inc. ("Rimkus") is writing to notify you of a recent event that may involve some of your information in connection with the handling of insurance claims. Although at this time there is no indication that your information has been fraudulently misused in relation to this event, we are providing you with information about the event, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? This past July, Rimkus noticed suspicious activity relating to certain Rimkus employees' email accounts. Rimkus quickly launched an investigation to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three Rimkus employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021, and issued emails to persons located within the Rimkus employees' email accounts. Rimkus promptly provided notice to each of the recipients of the erroneous emails.

Rimkus then worked with specialists to conduct a comprehensive review of information contained in the email accounts to determine what information was affected and to whom the information related. Upon completion of the third-party review, Rimkus then conducted a manual review of its records to confirm the identities of individuals affected by this event and their contact information to provide notifications. On or around December 30, 2021, Rimkus completed its initial review. Through the review, Rimkus determined that one of the email accounts contained information that was received from one or more of its clients in the course of business operations and included your personal information. On January 14, 2022, Rimkus notified this client of the incident and that it had been determined that your personal information may have been included within the contents of the email account, and with the client's approval and on its behalf, we are now notifying you.

What Information Was Involved? Rimkus' investigation determined that at the time of the event, your [**Variable2**] were stored within an impacted email account. To date, Rimkus has not received any reports of fraudulent misuse of anyone's information potentially impacted by this event.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event and to work with Rimkus in providing proper notifications.

While we are unaware of any fraudulent misuse of your information as a result of this event, as an additional precaution, Rimkus is offering you access to two years of complimentary credit monitoring services through Experian. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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 free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Protect Your Personal Information," which contains information on what you can do to safeguard against possible misuse of your information should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services.

For More Information. If you have additional questions, you may contact our toll-free dedicated assistance line at (855) 545-2581. This toll-free line is available Monday – Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding U.S. holidays). You may also write to us at 12140 Wickchester Lane, Suite 300, Houston, TX 77079

Sincerely,

John E. Orr
Senior VP, Marketing
Rimkus Consulting Group, Inc

Steps You Can Take to Protect Your Personal Information

Enroll in Identity Theft Protection Services

To help protect your identity, we are offering a complimentary twenty-four (24) month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: July 30, 2022 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [**Variable3**]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 288-8057 by April 4, 2022. Be prepared to provide engagement number # B023371 as proof of eligibility for the identity restoration services by Experian.

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 one-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, 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

Additional Information

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 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 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 3 Rhode Island residents impacted by this incident.

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/.