



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.

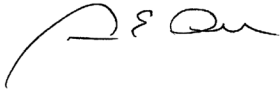
What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event, and implement additional security measures to protect your information and our systems.

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,

A handwritten signature in black ink, appearing to read "J. E. Orr". The signature is fluid and cursive, with a large initial "J" and "O".

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® IdentityWorksSM. 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>.

EXHIBIT B



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

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

<<b2b_text_2(Attention)>>
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Phishing Data Event

Dear valued customer:

Rimkus Consulting Group, Inc. (“Rimkus”) is writing to notify you of a recent event that may involve some personal information that belongs to you, your employees, or your customers (the “Personal Information”). Although at this time there is no indication that the Personal Information has been fraudulently misused in relation to this event, we wanted to inform you about the event and our ongoing response to it.

What Happened?

This past July, we observed suspicious activity relating to certain Rimkus employees’ email accounts. 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 of our employees’ email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021 (the “Event”).

Upon learning this information, we employed specialists to conduct a comprehensive review of the data contained in the impacted email accounts to determine what types of 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?

The Event impacted approximately <<b2b_text_3(impacted individuals)>> individual(s) associated with your organization or matters you assigned to us. Upon written request, we will securely send to you a list of affected individual(s) (the “Individual PI List”). Request for this secure transmission should be made to legal@rimkus.com.

Our investigation determined that at the time of the Event certain Personal Information was stored within an impacted email account. We have traced the Personal Information back to your organization as the original data owner or licensor. The Personal Information impacted by the Event includes <<b2b_text_1(name, data elements)>>.

To date, Rimkus has not received any reports of fraudulent misuse of any Personal Information potentially impacted by this Event.

How Are We Responding?

Upon learning of the Event, we immediately took steps to further secure our 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. Additionally, we would like to offer the affected individuals credit monitoring and call center access, as set forth below.

Provision of Notice To Affected Individuals

To assist you in your notification obligations, we have prepared a form notification letter for your consideration, attached as ***Exhibit A***. Additionally, we would like to offer those impacted by this Event access to two years of complimentary credit monitoring services through Experian, as well as identify restoration services, and call center access. Details of this offer and instructions on how to activate these services are enclosed with the form letter attached as ***Exhibit A***, and we encourage you to enclose these details, at your discretion, with your notice to those impacted by this Event (irrespective of whether you utilize the notice template letter we provide, or another notice letter of your own creation). Please contact legal@rimkus.com for the specific credit monitoring activation code(s) (as these are necessary for an affected individual to activate the complimentary credit monitoring services).

If you would prefer Rimkus to provide notice to potentially affected individuals and any necessary regulatory bodies on your behalf, please provide us with the following information, in writing at legal@rimkus.com, no later than 30 days from the date of this letter:

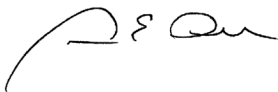
1. Authorization to mail notice to the potentially affected individuals associated with your organization on your behalf;
2. Authorization to provide those individuals with two years complimentary access to credit monitoring, as well as identify restoration services, and call center access;
3. Authorization to provide notice to regulatory bodies, if required; and
4. For each potentially affected individual in the Individual PI List, the complete address where you would like Rimkus to mail the notice letter (if a complete address is not contained in the Individual PI List, or if you would prefer an address differing from the one in the Individual PI List).

Rimkus will not take any further action on your behalf unless you provide the foregoing written authorization to do so.

For More Information

We want to cooperate with you in any way we can as you undertake your own notification obligations. Please feel free to reach out to us directly at (214) 244-3496. You may also write to Rimkus at 12140 Wickchester Lane, Suite 300, Houston, TX 77079 or legal@rimkus.com.

Sincerely,



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

EXHIBIT A

[Company letterhead]

[Date] (Format: Month Day, Year)

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

Re:

Dear [MemberFirstName] [MemberLastName]:

[COMPANY NAME] (“Company”) 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, Rimkus Consulting Group, Inc. (“RCG”), a company with which we do business, 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 the Company in the course of business operations that included [insert data elements]. On [insert date of mailing to organization], RCG notified us of the incident and that it had been determined that your [b2b_text_1(name, data elements)] 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 [b2b_text_1(name, data elements)] 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 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 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 [1-??-??-??]. 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 [insert company name and address].

Sincerely,

[Signatory]

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

[CONTACT legal@rimkus.com FOR ACTIVATION CODE(S)]

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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

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

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

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

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 21 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>.