LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

February 15, 2022

VIA EMAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP represents Reimbursement Consultants, Inc. ("RCI") in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. Nature of the Security Incident

RCI is a consulting firm specializing in recovering workers' compensation costs for insurance companies. In September of 2020, RCI learned of unusual activity involving an employee email account. Upon discovery, RCI immediately secured the account and its email environment, and launched an investigation. RCI engaged a digital forensics firm to assist with the process and to determine whether personal information may have been accessed or acquired without authorization. As a result of this investigation, RCI learned that the email account was accessed without authorization.

RCI then conducted a comprehensive review of the contents of the account and, on April 4, 2021, learned that the account contained personal information belonging to certain individuals. RCI then worked diligently to evaluate potentially impacted data elements and confirm identities of potentially impacted individuals. That process was completed on January 12, 2022. RCI then worked to identify current address information required to provide notice of the incident to such individuals.

2. Type of Information and Number of New Hampshire Residents Involved

The incident involved personal information for approximately **1** New Hampshire resident. The information involved in the incident may differ depending on the individual but may include name, social security number, driver's license number, medical information, or health insurance ID or information.

The affected individuals will receive a letter notifying them of the incident and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on February 15, 2021. A sample copy of the notification letter sent to the affected individuals is attached.

3. Measures Taken to Address the Incident

In response to the incident, RCI retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. RCI also reported this matter to the Federal Bureau of Investigation and to the Jefferson Parish Police Department in Louisiana.

Finally, RCI is notifying the affected individuals and providing them with steps they can take to protect their personal information. For the individuals whose Social Security numbers may have been impacted by the incident, RCI is also offering complimentary credit monitoring services.

4. Contact Information

RCI is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Sean Hoar at Sean.Hoar@lewisbrisbois.com.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Individual Notification Letter

Reimbursement Consultants, Inc.

Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

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

February 15, 2022

Re: Notice of Data Security Incident

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

Reimbursement Consultants, Inc ("RCI") is a consulting firm specializing in recovering workers' compensation costs for insurance companies. In certain situations, we receive information from insurers to assist in recovering workers' compensation costs associated with injured workers. RCI takes the privacy and security of your information very seriously. This is why we are writing to information you of a data security incident that may have affected your personal information, offering you complementary credit and identity monitoring services, as well as additional steps you can take to protect your personal information.

What Happened. In September of 2020, we learned of unusual activity involving an employee email account. We immediately secured the account and our email environment, and launched an investigation. We engaged a digital forensics firm to assist with the process and to determine whether personal information may have been accessed or acquired without authorization. As a result of this investigation, we learned that the email account was accessed without authorization. We then conducted a comprehensive review of the contents of the account and, on April 4, 2021, learned that the account contained personal information. We then worked diligently to evaluate potentially impacted data elements and confirm identities of potentially impacted individuals. That process was completed on January 12, 2022, at which time we learned that your information may have been affected. We then worked to identify current address information required to provide notification to the individuals whose personal information was contained within the impacted account.

What Information Was Involved. The impacted information may have included your name and the following information: <<Consolidated Data Elements>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. Additionally, we initiated measures to reduce the risk of a similar incident occurring in the future. We reported this matter to the Federal Bureau of Investigation and to the Jefferson Parish Police Department in Louisiana. RCI will provide complete cooperation that is necessary to hold the perpetrators accountable. We are also providing you with information about steps that you can take to help protect your personal information, and as an added precaution offering you identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<12 or 24 months>> of credit and Cyberscan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. To enroll, please log on to**: https://app.idx.us/account-creation/protect** or call **1-833-903-3648**. When prompted, please provide <CODE> to receive services. The deadline to enroll is May 15, 2022.

What You Can Do. You can enroll in the complimentary credit and identity monitoring services offered in this letter. In addition, you can review the resources provided on the following page for additional steps to protect your personal information.

For More Information. If you have questions or need assistance with enrollment, please call 1-833-903-3648 between 8:00 a.m. – 8:00 p.m. Central Time, Monday through Friday, except major U.S. holidays, or go to https://app.idx.us/account-creation/protect. We apologize for any worry or inconvenience that this may cause you.

Sincerely,

Lisa M. Gillespie
Vice President
Reimbursement Consultants, Inc.

Steps You Can take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act

Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

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

February 15, 2022

Re: Notice of Data Security Incident

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

Reimbursement Consultants, Inc ("RCI") is a consulting firm specializing in recovering workers' compensation costs for insurance companies. In certain situations, we receive information from insurers to assist in recovering workers' compensation costs associated with injured workers. RCI takes the privacy and security of your information very seriously. This is why we are writing to information you of a data security incident that may have affected your personal information and providing steps you can take to protect your personal information.

What Happened. In September of 2020, we learned of unusual activity involving an employee email account. We immediately secured the account and our email environment, and launched an investigation. We engaged a digital forensics firm to assist with the process and to determine whether personal information may have been accessed or acquired without authorization. As a result of this investigation, we learned that the email account was accessed without authorization. We then conducted a comprehensive review of the contents of the account and, on April 4, 2021, learned that the account contained personal information. We then worked diligently to evaluate potentially impacted data elements, confirm identities of potentially impacted individuals, and identify current address information required to provide notification to the individuals whose personal information was contained within the impacted account. That process was completed on January 12, 2022, at which time we learned that your information may have been affected. We then worked to identify current address information required to provide notification to the individuals whose personal information was contained within the impacted account.

What Information Was Involved. The impacted information may have included your <<Consolidated Data Elements>>.

What We Are Doing. As soon as we discovered this incident, RCI took the steps described above. Additionally, we initiated measures to reduce the risk of a similar incident occurring in the future. We reported this matter to the Federal Bureau of Investigation and to the Jefferson Parish Police Department in Louisiana. RCI will provide complete cooperation that is necessary to hold the perpetrators accountable. We are also providing you with information about steps that you can take to help protect your personal information, which can be found on the next page.

What You Can Do. You can review the resources provided on the following page and follow the steps outlined to protect your personal information.

For More Information. If you have questions, please call 1-833-903-3648 between 8:00 a.m. – 8:00 p.m. Central Time, Monday through Friday, except major U.S. holidays.

Sincerely,

Lisa M. Gillespie
Vice President
Reimbursement Consultants, Inc

Steps You Can take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act