LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

May 10, 2022

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Sarah Reames CPA in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

Sarah Reames CPA learned of unusual activity involving an employee email account on March 9, 2021. In response, Sarah Reames CPA took immediate steps to secure its digital environment and promptly launched an investigation. In so doing, Sarah Reames CPA engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. Given the type and quantity of data, significant time and resources were required to complete the review. On April 14, 2022, Sarah Reames CPA learned that certain personal information may have been impacted in connection with the incident. Sarah Reames CPA then worked diligently to identify address information required to effectuate notification which occurred on May 10, 2022. Notably, Sarah Reames CPA has no evidence of the misuse or attempted misuse of any potentially impacted information.

The information belonging to the one (1) Maryland resident that may have been impacted by this incident includes his/her Social Security Number.

2. Number of Maryland residents affected.

Sarah Reames CPA notified one (1) Maryland resident of this incident via first class U.S. mail on May 10, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Sarah Reames CPA discovered this incident, Sarah Reames CPA took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Sarah Reames CPA has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future. In addition, while Sarah Reames CPA is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Sarah Reames CPA is also providing complimentary identity protection services through IDX to notified individuals.

Sarah Reames CPA has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

4. Contact information.

Sarah Reames CPA remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Lewis Brisbois.

Very truly yours,

Allen Sattler

Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

Sarah Reames CPA
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

May 10, 2022

Re: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

I am writing to inform you of a data security incident that may have involved your personal information. At Sarah N. Reames, CPA, PLLC ("Sarah Reames CPA") we take the privacy and security of personal information in our possession very seriously. This is why I am writing to notify you of this incident and provide information on steps you can take to protect your information, including enrolling in the complimentary identity monitoring services Sarah Reames CPA is making available to you.

What Happened? Sarah Reames CPA learned of unusual activity involving an employee email account. Upon discovering this activity, we immediately began an investigation and took steps to secure our email system. We also engaged an independent digital forensics firm to conduct an investigation which revealed that the employee's email account may have been accessed without authorization. We then promptly commenced a thorough search of the contents of the email account to identify whether any personal information was contained therein. Given the type and quantity of data, significant time and resources were required to complete the review. On April 14, 2022, we learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. We then worked diligently to identify the current mailing addresses for each potentially impacted individual in order to notify them of the incident and provide guidance on steps to take to protect such information.

What Information Was Involved? The information may have involved your name and <<variable text>>.

What We Are Doing? As soon as we discovered this incident, we took the measures referenced above. We also enhanced the security of our network and email systems to help prevent a similar incident from occurring in the future. We are also providing you guidance on steps you can take to protect your personal information.

In addition, we are offering identity theft protection services through IDX – a data breach and recovery services expert – at no cost you. The IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

With this protection, IDX will help you resolve issues if your identity is compromised. Please note that we do not have any evidence indicating that your information has been misused, but are providing these services as an added precaution.

To activate your membership, visit https://app.idx.us/account-creation/protect or call 1-800-939-4170 and provide the activation code listed at the top of this letter. The deadline to enroll in the membership is August 10, 2022.

2548 Plantation Center Drive, Suite B • Matthews, NC 28105 • Phone: 704-362-2272

What Can You Do? You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter. In addition, you can enroll in the complimentary IDX membership to receive credit monitoring and identity theft protection services outlined above.

For More Information: If you have questions or need assistance in enrolling in the complimentary identity theft protection services, please contact IDX at 1-800-939-4170**.** IDX representatives are available to assist you Monday through Friday from 9 am – 9 pm Eastern Standard Time. We have also provided more resources and contact information for agencies which can provide assistance in taking steps to further protect your information in the attached guidance included with this letter.

We take your trust in us and the protection of your information very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Sarah N Reames

SARAH N. REAMES, CPA/PFS
PERSONAL FINANCIAL SPECIALIST

Steps You Can Take to Further Protect Your 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 can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	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	Maryland Attorney General	New York Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	Bureau of Internet and Technology Resources
Washington, DC 20580	Baltimore, MD 21202	28 Liberty Street
consumer.ftc.gov, and	oag.state.md.us	New York, NY 10005
www.ftc.gov/idtheft	1-888-743-0023	1-212-416-8433
1-877-438-4338		

North Carolina Attorney General	Rhode Island Attorney General	Washington D.C. Attorney General
9001 Mail Service Center	150 South Main Street	441 4th Street, NW
Raleigh, NC 27699	Providence, RI 02903	Washington, DC 20001
ncdoj.gov	http://www.riag.ri.gov	oag.dc.gov
1-877-566-7226	1-401-274-4400	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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.