LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 5000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

May 27, 2020

VIA E-MAIL
Gordon J. MacDonald, Attorney General
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Yount, Hyde & Barbour, P.C. ("YHB"), an accounting and consulting firm headquartered in Winchester, Virginia. As described in greater detail below, this letter is being submitted on behalf of YHB pursuant to N.H. Rev. Stat. § 359-C:19-21, because the personal information of one New Hampshire resident may have been affected by a recent data security incident experienced by YHB. The incident may have involved unauthorized access to one resident's name and Social Security number.

1. Nature of the Incident. On February 13, 2020, YHB discovered unusual activity in an employee's email account. YHB immediately took steps to secure its email system and launched an investigation with the assistance of a leading digital forensics firm to determine whether additional email accounts may have been impacted and whether any personal information may have been accessed without authorization. Through this investigation, YHB learned that a limited number of YHB employee email accounts may have been subject to unauthorized access between approximately October 15, 2019 and January 23, 2020. Upon learning this information, YHB launched a data review project to determine whether the accounts contained personal information. On April 24, 2020, the data review project resulted in the identification of individuals whose personal information was contained within one or more of the accounts and therefore may have been accessed without authorization. YHB then worked to identify up-to-date address information required to notify potentially affected individuals.

2. New Hampshire Residents Notified. On May 14, 2020, YHB confirmed that the personal information of the above-referenced New Hampshire resident was contained within one or more of the impacted email accounts. On May 27, 2020, YHB notified one New Hampshire resident via the attached sample letter.

3. Steps Taken Relating to the Incident. YHB has implemented enhanced security measures in order to help prevent a similar incident from occurring in the future, including a universal password

change, internal email policy revisions, and disabling email forwarding rules. YHB is also in the process of rolling out additional security measures, such as Advanced Threat Protection through Microsoft and multi-factor authentication. In addition, YHB reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. The notified resident is also being offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Kroll, a global leader in risk mitigation and response.

4. Contact Information. If you have any questions or need additional information, please do not hesitate to contact me at 720.292.2052 or via email at Alyssa.Watzman@lewisbrisbois.com.

Very truly yours,

/s/ Alyssa Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

Re: Notice of Data Security Incident

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

We are writing to inform you of a data security incident experienced by Yount, Hyde & Barbour ("YHB") that may have affected your personal information. YHB takes the privacy and security of all information very seriously and deeply regrets any concern that this incident may cause. We are writing to notify you of this incident, to offer you complimentary credit monitoring and identity protection services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On February 13, 2020, YHB discovered unusual activity in an employee's email account. YHB immediately took steps to secure its email system and launched an investigation with the assistance of a leading digital forensics firm to determine whether additional email accounts may have been impacted and whether any personal information was accessed without authorization. Through this investigation, YHB learned that a limited number of YHB employee email accounts may have been subject to unauthorized access between approximately October 15, 2019 and January 23, 2020. On April 24, 2020, our investigation determined that your information was contained in the impacted accounts and therefore may have been viewed or accessed without authorization. YHB then worked to identify up-to-date address information required to notify you.

Please note that this incident was limited to information transmitted via email and did not affect any other information systems. Moreover, we are not aware of the misuse of any of your personal information.

What Information Was Involved? The information may have included your <<insert variable text>>.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above. We also implemented enhanced security measures in order to help prevent a similar incident from occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. Out of an abundance of caution, we are also providing you with information about steps you can take to help protect your information and complimentary credit monitoring and identity protection services through Kroll, a global leader in risk mitigation and response. These services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your personal information. In addition, we recommend that you enroll in the complimentary credit monitoring and identity protection services being offered through Kroll. Enrollment instructions and a description of the services being provided are included with this letter.

For More Information. If you have questions or need assistance, please contact Kroll at <<insert number>>, Monday through Friday from 9 a.m. to 6:30 p.m. Eastern Time. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

R. Curtis Thomson, CPA, CITP, CISA
Technology Principal
Yount, Hyde & Barbour

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 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 https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.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 90 days. 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. 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. There is no charge to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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 others. 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.

As referenced above, we have secured the services of Kroll to provide credit monitoring and identity protection services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services[1] include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit <<ID Monitoring URL>> to activate and take advantage of your credit monitoring and identity protection services.

You have until <<Date>> to activate your credit monitoring and identity protection services.

Membership Number: <<Member ID>>

If you have questions, please call <<Phone Number>>, Monday through Friday from 9 a.m. to 6:30 p.m. Central Time.

Take Advantage of Your Services

You've been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for covered, out-of-pocket expenses totaling up to $1 million for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.