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 1, 2017

File No. 39395.02

VIA E-MAIL

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: attorneygeneral@doj.nh.gov

Re: Data Security Incident

Dear Attorney General Foster:

I represent King McNamara Moriarty ("KMM"), an accounting firm located in Norwood, Massachusetts. This letter is being sent pursuant to N.H. Rev. Stat §§ 359-C:19-359-C:21 because KMM determined on December 13, 2016 that personal information of 76 New Hampshire residents may have been involved in a data security incident. The information which may have been involved includes tax return information, including names, addresses, dates of birth, and Social Security numbers.

KMM believes this data security incident is connected to a malicious hacking incident which KMM was the victim of several months ago. When that occurred, KMM immediately engaged a digital forensics firm to contain the matter, identified and notified the affected clients, and offered them free credit and identity monitoring services. At that time, KMM was informed by the forensics firm that the incident was completely contained and the affected clients had been identified. Unfortunately, KMM later detected a suspicious file on its network and retained a second digital forensics firm to investigate. On December 13, 2016, the second digital forensics firm confirmed that certain additional client data—which was undetected in the previous digital forensics investigation—may have been accessed without authorization. KMM has notified the police, the Internal Revenue e-File Services Department, and the Internal Revenue Service/Criminal Investigation (IRS/CI) of the incident in an attempt to prevent any fraudulent activity.

KMM has also notified the affected consumers via the attached letter. As referenced in the letter, KMM is offering 12 months of credit and identity monitoring services through Kroll, a risk mitigation company. Please contact me if you have any questions.

Sincerely,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DEA:SBH
Encl.: Consumer notification letter

King McNamara Moriarty

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

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

Subject: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

I am writing to inform you of a data security incident that may have affected your personal information. We take the privacy and security of your information very seriously. This is why we are contacting you, offering you credit and identity monitoring services, and informing you about steps that can be taken to protect your personal information.

What Happened? We were victims of a malicious hacking incident several months ago. When that occurred, we immediately engaged a digital forensics firm to contain the matter and to identify the affected clients so that we could notify and offer credit and identity monitoring services to them. We were informed at the time that the incident was completely contained and that all affected clients had been identified. On June 23, 2016 we notified the affected clients and offered credit and identity monitoring services to them. Unbeknownst to us, unfortunately, all affected clients had not been identified. As it turned out, on October 24, 2016, after detecting a suspicious file on our network, we retained a different digital forensics firm to conduct an additional forensics investigation into the matter. The forensics investigation was complex and was completed in December. On December 13, 2016, the digital forensics firm confirmed that certain additional client data - which was undetected in the previous digital forensics investigation - may have been accessed without authorization. It appears that your data was among that which may have been accessed without authorization. While we have no evidence that the data was actually misappropriated, out of an abundance of caution, we are notifying you of the incident, and are offering you credit and identity monitoring.

What Information Was Involved? The following information appears to have been accessed: tax return information which included names, addresses, dates of birth, and Social Security numbers.

What We Are Doing: As soon as we detected that someone may have accessed client files without authorization, which were not detected in the previous digital forensics investigation, we engaged another digital forensics firm to conduct an investigation. We also notified the Internal Revenue e-File Services Department and the Internal Revenue Service/Criminal Investigation (IRS/CI) in an attempt to prevent fraudulent returns from being accepted or refunds issued. We are also providing you information about steps you can take to protect your personal information, and are offering you credit and identity monitoring services for 12 months at no cost to you. We are also enhancing the security of our systems, making it more difficult for similar incidents to occur in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. You can also enroll in the services we are offering through Kroll, a global leader in risk mitigation and response, to protect your identity for 12 months at no cost to you. 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. Your services start on the date of this notice and can be used at any time during the next 12 months. They will include credit monitoring, web watcher and identity consultation and restoration. Visit **kroll.idMonitoringService.com** to take advantage of your services. Your membership number is **<<Member ID>>**. To receive credit services by mail instead of online, please call **1-855-656-6588**.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, call **1-855-656-6588** 9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday. Kroll's licensed investigators are standing by to assist you. Please have your membership number ready.

If you haven't already done so, I also encourage you to complete IRS Form 14039, Identity Theft Affidavit which you can obtain at http://www.irs.gov/pub/irs-pdf/f14039.pdf, and then mail or fax it to the IRS according to instructions on the form. Please contact us should you need assistance filing Form 14039. If you have other identity theft/tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

We are grateful for your business and your trust. Please accept my sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Joseph B. Moriarty, CPA
Managing Partner

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:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.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: In some US states, 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. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 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, Federal Trade Commission 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 Federal Trade Commission 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			