FREEMAN MATHIS & GARY
A LIMITED LIABILITY PARTNERSHIP

100 Galleria Parkway
Suite 1600
Atlanta, Ga. 30339-5948

Tel: 770.818.0000
Fax: 770.937.9960

www.fmglaw.com

David A. Cole
Partner

Writer's Direct Access
770.818.1287

dcole@fmglaw.com

June 11, 2019

VIA U.S. MAIL & EMAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice of Breach in the Security of Personal Information

Dear Attorney General:

I represent Hood & Associates CPAs, PC ("Hood & Associates"), an Oklahoma-based CPA firm. This letter is being provided pursuant to N.H. Rev. Stat. § 359-C:20, which requires that your office be notified in the event of a breach in the security of confidential personal information affecting New Hampshire residents.

Hood & Associates recently learned that, from approximately March 12, 2018 through March 24, 2019, its firm computer network and email accounts were accessed without its knowledge by an unauthorized individual not affiliated with Hood & Associates. Upon discovery, Hood & Associates worked with legal counsel and computer forensic specialists to investigate the incident. Hood & Associates cannot confirm with certainty which files or data may have been accessed or acquired during that time, but it is possible that some clients' tax returns and other documents containing personal information may have been accessed or acquired. This information may have included full names, addresses, Social Security numbers, dates of birth, driver's license or government identification card numbers, and/or financial account numbers. As a result, Hood & Associates is notifying all potentially affected individuals about this incident out of an abundance of caution. Among the 7,013 potentially affected individuals, only one is a resident of New Hampshire.

Please know that Hood & Associates takes the protection of its clients' personal information seriously and is taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents from happening. Hood & Associates also has made additional investments in enhanced monitoring, hardware, software, and staff training to further improve the protection of its clients' data, including an enhanced firewall and 24/7 monitoring.

Hood & Associates has reported the incident to law enforcement and will cooperate with any investigation. It is also reviewing its network and email accounts to ensure that documents containing personal information are encrypted and accessible only through dual-factor authentication. Going forward, Hood & Associates will continue to review its network, policies, and procedures to identify any additional ways to help prevent a future incident.

In addition, written notice is being mailed to the affected New Hampshire resident on June 11, 2019. A sample copy of the notice has been enclosed for your records. As an added precaution, Hood & Associates is offering the New Hampshire resident 12-months of free identity theft protection services through *my*TrueIdentity, provided by TransUnion Interactive, a subsidiary of TransUnion®. The notice to the affected individual includes instructions on the use of this product.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if you have any additional questions or need further information, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

David A. Cole

DAC/mk
Enclosure

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

Thank you for using Hood & Associates CPAs, PC ("Hood & Associates") for your tax and accounting services. We take our clients' privacy seriously, and as part of that commitment, we are sending you this letter to make you aware of a recent incident that may affect your personal information.[1] Please read this letter carefully.

What Happened

At our offices, we maintain technological safeguards to protect the security and privacy of our clients' information. Unfortunately, we live in a technology world where even the best systems are vulnerable. In that regard, we have recently learned that, from approximately March 12, 2018 through March 24, 2019, our firm's computer network and email accounts were accessed without our knowledge by an unauthorized individual not affiliated with Hood & Associates. Upon discovery, we worked with legal counsel and leading computer forensic specialists to investigate the incident. We cannot confirm with certainty which files or data may have been accessed or acquired during that time, but we believe it is possible that some clients' tax returns and other documents containing their personal information may have been accessed or acquired. As a result, we are notifying all potentially affected individuals about this incident out of an abundance of caution.

What Information Was Involved

Based on our investigation, it is possible that there may have been unauthorized access to or acquisition of your tax returns or other documents containing your personal information, including your full name, address, Social Security number, date of birth, driver's license or government identification card number, and/or financial account number(s).

What We Are Doing

Please know that we take the protection of our clients' personal information seriously and are taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent future incidents from happening. We have reported the incident to law enforcement and will cooperate with any investigation. We also have made additional investments in enhanced monitoring, hardware, software, and staff training to further improve the protection of our clients' data, including an enhanced firewall on our network and 24/7 monitoring. We are also reviewing our network and email accounts to ensure that documents containing personal information are encrypted and accessible only through dual-factor authentication. Going forward, we will continue to review our network, policies, and procedures to identify any additional ways to help prevent a future incident.

[1] Certain employees of Hood & Associates are also registered representatives for the sale of securities products of Royal Alliance Associates, Inc., a registered securities broker-dealer.

What You Can Do

Please note that, at this time, we are not aware of any misuse of our clients' information. Nonetheless, we recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institution or call the number on the back of your payment card. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

As an additional precautionary measure to help protect your identity, we are offering one year of identity theft protection services through *my*TrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion®, at no cost to you. Please refer to the enclosed documentation for further instructions on how to enroll in these services.

For More Information

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, you may contact us through our dedicated hotline at 877-202-9536, Monday through Friday, from 9 am to 9 pm Eastern Time (except holidays).

Sincerely,

Paul Hood, CPA

Additional Steps to Help Protect Your Information

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. Starting September 21, 2018, you can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. If you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, (502) 696-5300.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, (888) 743-0023.
- **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.

- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know Your Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, which you can read about by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf and https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (your "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (10) You may seek damages from violators; and (11) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.

TransUnion

Activation Code: <<Activation Code>>

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)