MARSHALL DENNEHEY
WARNER COLEMAN & GOGGIN
ATTORNEYS-AT-LAW WWW.MARSHALLDENNEHEY.COM
A PROFESSIONAL CORPORATION
2000 Market Street, Suite 2300 · Philadelphia, PA 19103
(215) 575-2600 · Fax (215) 575-0856

PENNSYLVANIA
Allentown
Doylestown
Erie
Harrisburg
King of Prussia
Philadelphia
Pittsburgh
Scranton
NEW JERSEY
Cherry Hill
Roseland
DELAWARE
Wilmington
OHIO
Cincinnati
Cleveland
FLORIDA
Ft. Lauderdale
Jacksonville
Orlando
Tampa
NEW YORK
Long Island
New York City
Westchester

Direct Dial: 215-575-2615
Email: djshannon@mdwcg.com

June 20, 2017

Via Email: attorneygeneral@doj.nh.gov
Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: David Turrentine & Associates, Inc.
Our File No. 41105.00110

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20(I)(b), we are writing to notify you of a data security incident involving four New Hampshire residents. We are submitting this notification on behalf of our client, David Turrentine & Associates, Inc.

Nature Of The Security Breach

David Turrentine & Associates, Inc. is an accounting firm located in Chicago, Illinois. On or about March 30, 2017, David Turrentine & Associates, Inc. became aware that it may have been the victim of a cyber-attack by which an unknown third party was able to access the firm's computer network and some of its clients' personal information. Based on the internal investigation of this matter, the client information potentially at risk of being accessed included first and last names, home addresses, social security numbers, and 2015 tax return information, including compensation data. While the vast majority of the 2016 tax returns that the firm prepared have been successfully transmitted and accepted by the IRS, a number of the firm's clients have been advised that fraudulent tax returns were filed with the IRS using their social security number. To the firm's knowledge, none of its clients have lost any of their refunds, or have experienced any adverse consequences to their finances as a result of this incident.

The New Hampshire residents involved in this incident were notified of this incident by email on March 31, 2017. A follow-up letter that includes instructions for enrolling in free credit monitoring services provided by Equifax and information on how to monitor and safeguard credit will be forwarded as soon as possible. A copy of the initial correspondence and follow-up letter is attached hereto.

Steps Taken Relating To The Incident

Upon learning of the cyber attack, David Turrentine & Associates, Inc. took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better understanding of what had taken place and how. The firm reported the incident to local law enforcement, and they are investigating. This notification was not delayed as a result of a law enforcement investigation. The firm has also engaged the services of an independent computer forensic firm to ensure that the computer system is now secure. The firm is also in the process of reviewing its internal policies and data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring in the future.

David Turrentine & Associates, Inc. has also arranged to have Equifax protect the affected individuals' identity for one year at no cost to them through its Credit Watch ™ Gold credit monitoring and identity theft protection service. This service offers additional layers of protection including credit monitoring and a $25,000 identity theft insurance policy.

Should you need additional information regarding this matter, please contact me.

Very truly yours,

D.S.

DAVID J. SHANNON

DJS:jl
Encl.

Dear Client:

As many of you may have heard from the media, once again there have been a number of fraudulent tax returns filed with the Internal Revenue Service this season. This fraud is generally conducted by individuals attempting to obtain and steal taxpayers' refunds to which they are not entitled. While the vast majority of the 2016 tax returns prepared by my firm have been successfully transmitted and accepted by the IRS, a number of my clients have been advised that fraudulently prepared tax returns have been filed with the IRS using their social security number. To my knowledge none of my clients have in fact lost any of their refunds, and none have experienced any adverse consequences to their finances resulting from this type of fraudulent activity.

In order to protect yourself, I recommend ordering a credit report and continuing to review all your financial accounts. U.S. citizens are entitled to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

If you learn that a 2016 tax return has been filed using your social security number, it will likely be necessary that you file a paper return (rather than an electronic filing) for 2016. If this is the case, my office will provide you with a paper return with filing instructions. Unfortunately, the authentic paper return that replaces the previously filed fraudulent return will take more time for the IRS to process. It is currently estimated that it will take nine weeks for the IRS to process these paper returns and issue refunds.

As a result of the additional time required to make sure that clients' accounts are secure, and tax returns are properly filed, it may be necessary for me to file an extension for you this tax season. Extensions prepared and transmitted by my firm incur no additional charge.

In light of this fraudulent trend, I will be assisting clients with obtaining IP PINs (Identity Protection Personal Identification Number) issued by the IRS. The IRS provides this IP PIN to be used in conjunction with your social security number as an added security measure to ensure that a fraudulent return ***cannot be filed***. Subsequently, the IRS will issue you a new IP PIN every year to be used when filing your return.

Here are links to the IRS website with additional information regarding this issue:

https://www.irs.gov/uac/taxpayer-guide-to-identity-theft

https://www.irs.gov/individuals/identity-protection-tips

In today's internet climate, be assured that David Turrentine & Associates, Inc. is taking extensive measures to protect your information.

Thank you for your patience and understanding as I work with you this tax season.

Please feel free to contact me with any questions or concerns.

Sincerely,

David Turrentine, EA

David Turrentine & Associates, Inc.
Individual and Business Tax Preparation
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<First_Name>><<Middle_Name>><<Last_Name>>
<<Address1>>
<<Address2>>
<<City>>< <ST>>< <ZIP>>

<<Date>>

Dear <<First_Name>><<Last_Name>>:

Please allow this letter to serve as a follow-up to my email correspondence dated March 31, 2017 in which I informed you of a incident at David Turrentine & Associates, Inc. that involved potential fraudulent activity with the filing of tax returns. I am sending this follow-up letter to provide you with additional information regarding steps that you can take to safeguard your identity and to offer complimentary credit monitoring and identity theft protection.

What Happened

On or about March 30, 2017, I became aware that David Turrentine & Associates, Inc. may have been the victim of a cyber-attack by which an unknown third party was able to access my firm's computer network and some of my clients' personal information. The investigation of this incident is ongoing, however, indications are that unauthorized access may have occurred. While the vast majority of the 2016 tax returns that my firm prepared have been successfully transmitted and accepted by the IRS, a number of my clients have been advised that fraudulent tax returns were filed with the IRS using their social security number. To my knowledge, none of my clients have lost any of their refunds, or have experienced any adverse consequences to their finances as a result of this incident.

What Information Was Involved

Based on the internal investigation of this matter, the client information potentially at risk of being accessed included first and last names, home addresses, social security numbers, and 2015 tax return information, including compensation data.

What I Am Doing

Everything I can. I take the privacy and protection of my clients' personal information very seriously and I deeply regret that this incident occurred. I took steps to address this incident promptly after it was discovered, including undertaking an internal investigation of the matter in order to develop a better understanding of what had taken place and how. I reported the incident to local law enforcement, and they are investigating. This notification was not delayed as a result of a law enforcement investigation. I have also engaged the services of an independent computer forensic firm to ensure that the computer system is now secure. I am in the process of reviewing my firm's internal policies and data management protocols and have implemented enhanced security measures to help prevent this type of incident from recurring in the future.

Securing your personal information is important to me. As a precautionary measure to help better protect your credit file from potential misuse, I have partnered with Equifax ® to provide its Credit Watch ™ Gold credit monitoring and identity theft protection product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to $25,000 Identity Theft Insurance [1] Coverage, automatic fraud alerts[2] , access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00a.m. to 8:00p.m. Eastern, Monday through Friday, before June 10, 2018.

You must complete the enrollment process for Equifax Credit Watch™ Gold by September 15, 2017. I urge you to consider enrolling in this product, at my expense, and reviewing the Additional Resources enclosed with this letter.

What You Can Do

You can take the following steps to guard against identity theft and fraud:

- Register for the complimentary credit monitoring services provided by David Turrentine & Associates, Inc. at no cost to you, as discussed in this letter.

- As a general precaution we recommend that you review your credit and debit card account statements as soon as possible to determine if there are any discrepancies or unusual activity listed.

- Remain vigilant and continue to monitor your bank and credit card statements for unusual activity going forward. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, call the bank that issued your credit or debit card immediately.

- Carefully check your credit reports for accounts you did not open or for inquiries from creditors that you did not initiate. If you see anything that you do not understand, call the credit agency immediately. As part of the complimentary protection, you may discuss your concern with any of the three primary credit agencies – Equifax, Experian, and TransUnion (see enclosures for contact information).

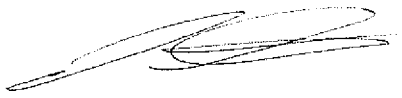
- Place a "fraud alert" or "security freeze" on your credit file. Information about these options for your credit file, along with instructions for activating these options, can be found in the enclosed reference materials, or by contacting one of the three credit agencies noted above.

- Review the enclosed "Information About Identity Theft Protection" reference guide, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding your identity theft protection.

For More Information

If you have questions about the information in this letter, please contact me by dialing 773-509-1798. Personally, I will make sure that I do everything I can for you to resolve any issues resulting from this incident and to guard against any potential use of your information. Once again, the privacy and protection of your information is a matter I take very seriously and I sincerely apologize for any concern that this may cause you.

Sincerely,



David Turrentine, EA

EQUIFAX®

Activation Code: < Credit Monitoring Code>

About the Equifax Credit Watch™ Gold credit monitoring and identity theft protection product

Equifax Credit Watch will provide you with an alert to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Equifax credit file monitoring and alerts of key changes to your **Equifax** credit report
- Wireless alerts and customizable alerts available (available online only) Data charges may apply.
- Access to your Equifax credit report
- Up to $25,000 in identity theft insurance [1]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.
- Automated renewal functionality of a 90 day fraud alert placement[2] (available online only)
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.
- Call <dynamic phone # by product/partner>, <dynamic contact hours by product/partner> for assistance.

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/gold

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

[1]Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age).

[2]The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

Information about Identity Theft Prevention

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, 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 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for 7 years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.