



Teal, Becker & Chiaramonte™  
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Fax: (603) 271-2110  
email: attorneygeneral@doj.nh.gov

March 23, 2018

Office of the Attorney General  
State of New Hampshire  
33 Capitol Street  
Concord, NH 03301

Dear Sir/Madam:

On behalf of Teal Becker & Chiaramonte, CPAs, PC ("TBC"), I am writing to notify you of a breach of security of personal information involving 17 New Hampshire residents.

#### **NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS**

On February 21, 2018, we were alerted by New York State Department of Taxation and Finance ("NYSDTF") that approximately 50 tax returns were filed for 2017 under TBC's electronic filing ID number for existing TBC clients with tax information similar to the client's 2016 tax information. We immediately contacted the IRS which confirmed similar activity and we suspended the filing of electronic tax returns.

To date, expert and forensic investigations have revealed that a routine test was performed on November 29, 2017 on our data restoration procedures in an offsite, completely separate, cloud-based location maintained by a third party. The data at this separate location was the subject of a ransomware attack. We immediately directed that our outside information technology expert conduct an investigation which determined at that time that there was no evidence of unauthorized download or copied information.

#### **NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED**

The 17 residents will shortly receive notice by mail. We have included a copy of the notice to the affected Virginia resident.

#### **STEPS TBC HAS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT**

We take our responsibilities to protect our client's information **very** seriously. We have been working with multiple external network security experts ever since to determine the source and the extent of the breach. This investigation is ongoing. Promptly after the NYSDTF notified us in mid-February as noted above, we consulted with the prior information technology expert and, in addition, engaged another information technology and forensic expert to investigate this matter and provide a comprehensive assessment of our own electronic systems and network and its security. We have been

advised by the experts that our network, which was never connected to the breached location, shows no indication of a significant vulnerability or a past compromise. The investigation by the new technology and forensic expert is continuing in order to determine the source and scope of any prior breach against the separate location. They are also assisting us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place and to recommend enhancements as appropriate.

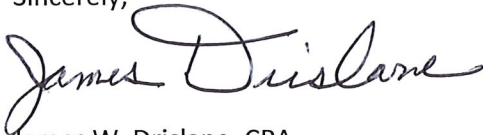
We have reported this incident to federal law enforcement agencies. We are working with the IRS and the NYSDTF to safeguard the tax information for returns that were filed and will be filed.

In addition, we are committed to helping those people who may have been impacted by providing the affected individuals with access to **Triple Bureau Credit Monitoring** services at no charge; separate services for impacted minors are being provided. In addition, we are providing proactive fraud assistance to help with any questions that those individuals might have. These services will be provided by **CyberScout** a company that specializes in identity theft education and resolution.

#### CONTACT INFORMATION

If you have any questions or need further information, please call Michele Auricchio, CPA MBA, Firm Administrator, at 518-456-6663.

Sincerely,

A handwritten signature in dark ink, reading "James Drislane". The signature is fluid and cursive, with the first name "James" and last name "Drislane" clearly legible.

James W. Drislane, CPA

Managing Shareholder

Enclosure





Teal, Becker & Chiaramonte™  
CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Date

**FORM OF NOTICE TO AFFECTED INDIVIDUALS**

Name

Address

Address

Address

Dear:

**Notice of Data Breach**

**Please read this letter in its entirety.**

We take security and the safe guarding of your personal information seriously at Teal, Becker & Chiaramonte, CPAs, P.C. Unfortunately, we are contacting you about an incident that may have involved that information.

**What Happened?**

On February 21, 2018, we were alerted by New York State Department of Taxation and Finance ("NYSDTF") that approximately 50 tax returns were filed for 2017 under TBC's electronic filing ID number for existing TBC clients with tax information similar to the client's 2016 tax information. We immediately contacted the IRS which confirmed similar activity and we suspended the filing of electronic tax returns.

We have been working with multiple external network security experts ever since to determine the source and the extent of the breach. This investigation is ongoing.

To date, the investigations have revealed that a routine test was performed on November 29, 2017 on our data restoration procedures in an offsite, completely separate, cloud-based location maintained by a third party. The data at this separate location was the subject of a ransomware attack. We immediately directed that our outside information technology expert conduct an investigation which determined at that time that there was no evidence of unauthorized download or copied information.

Promptly after the NYSDTF notified us in mid-February as noted above, we consulted with the prior information technology expert and, in addition, engaged another information technology and forensic expert to investigate this matter and provide a comprehensive assessment of our own electronic systems and network and its security. We have been advised by the experts that our network, which was never connected to the breached location, shows no indication of a significant vulnerability or a past compromise. The investigation by the new technology and forensic expert is continuing in order to determine the source and scope of any prior breach against the separate location.

We have reported this incident to federal law enforcement agencies. We are working with the IRS and the NYSDTF to safeguard your tax information for returns that were filed and will be filed.

We have resumed e-filing tax returns. If your e-filed tax return is rejected due to a data theft (or for any other reason), the valid return will have to be paper-filed and you may need to file IRS Form 14039 with the return. If we find any issues with your 2017 return when we e-file it, we will promptly inform you.

7 Washington Square, Albany, NY 12205 Ph: (518) 456-6663 | Fax: (518) 456-3975 [www.tbccpa.com](http://www.tbccpa.com)

### What Information was Involved?

The compromised data may have included personally identifiable information (PII) with some combination of your name, address, social security number and financial information.

**We are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.**

### What is TBC doing to address this situation?

TBC immediately engaged appropriate IT and forensic experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place and to recommend enhancements as appropriate. In addition, we are committed to helping those people who may have been impacted by this unfortunate situation. That's why TBC is providing you with access to **Triple Bureau Credit Monitoring**\* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have. These services will be provided by **CyberScout** a company that specializes in identity theft education and resolution.

### How do I enroll for the free services?

To enroll in **Credit Monitoring**\* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. **When prompted please provide the following unique code to receive services:**

<adult1>

<code1>

<adult2>

<code2>

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with your unique code.

### What You Can Do

If you choose not to enroll in the credit monitoring services, **we are strongly urging you to consider the following:**

**If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:**

**Experian (1-888-397-3742)**  
P.O. Box 4500  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

**Equifax (1-800-525-6285)**  
P.O. Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)

**TransUnion (1-800-680-7289)**  
P.O. Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)

**Also, should you wish to obtain a credit report and monitor it on your own:**

**IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.

**Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.**

\* Services marked with an "\*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



Be sure to promptly report any suspicious activity to TBC or CyberScout.
--

### **Other Important Information**

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

Due to credit monitoring tools not being available for minor children since a child should not have a credit file before age 18, credit monitoring services are not a practical solution. For this reason, TBC is providing special services geared towards any impacted minor dependents. This includes assistance with placing a Protected Consumer Credit File Freeze with the credit reporting agencies, if you are in a state where that service is offered. Fees may apply depending on the state in which the minor resides. If your state does not offer a Protected Consumer Credit File Freeze, then there are other proactive steps that can be taken. These services will also be provided by CyberScout.

<minor name>	<minor code>	<minor name2>	<minor code2>
<minor name3>	<minor code3>	<minor name4>	<minor code4>

### **For More Information**

While CyberScout should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with us regarding this incident. If so, please call Michele Auricchio at 518-456-6663 from 9:00AM to 5:00PM Eastern Time, Monday through Friday.

At TBC we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

James W. Drislane, CPA  
Managing Shareholder