MULLEN COUGHLIN LLC

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 27, 2017

VIA U.S. 1st CLASS MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

Our office represents John D. Williamson, Certified Public Accountant ("John Williamson"), PMB 118, 1278 Glenneyre, Laguna Beach, California 92651. We are writing to provide you with notice of an event that may impact the security of personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, John Williamson does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Background

On the morning of February 10, 2017 John Williamson discovered that his vehicle had been stolen during the overnight hours of February 9 into February, 10, 2017. John Williamson quickly reported this incident to local law enforcement and has been cooperating with their investigation. Located inside of the vehicle's trunk at the time of the theft were two password protected laptop computers owned by John Williamson containing tax software for his personal tax clients. That software

electronically stored personal tax information including the name, address, Social Security number and date of birth for all of the persons listed on tax returns (including clients' spouses and dependents). Depending upon whether bank account information was provided by a client to John Williamson for purposes of tax refund Direct Deposit, this type of information may also have been stored within the tax software contained on the laptop computers. One of the laptops possibly stored client information relating to tax years as far back as 2010. John Williamson has no evidence that the laptops were targeted by the responsible actor or that the information stored on the laptops at the time they were stolen was accessed or acquired by the responsible actor or any other unauthorized individual.

Notice to New Hampshire Resident

Based upon a review of his internal records, John Williamson determined that the electronic data stored on the two stolen laptops potentially includes personal information for certain current and former clients and their spouses and dependents. John Williamson mailed written notice of this incident to one (1) New Hampshire resident on February 24, 2017, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and to Be Taken

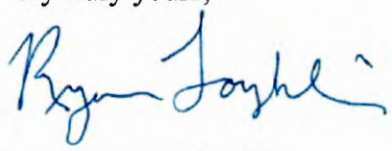
John Williamson is offering all individuals impacted by this incident access to 2 free years of credit monitoring and identity protection services through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, John Williamson is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, resources on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Notice is also being provided to other state regulators as necessary.

John Williamson has implemented a new policy prohibiting the storage of sensitive client data on portable electronic devices. He has also reset and strengthened relevant user account passwords relating to his practice and will be increasing the number of passwords needed to access internal tax software.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:ncl
Enclosure

Exhibit A

John Williamson
CERTIFIED
PUBLIC
ACCOUNTANT

Processing Center • P.O. BOX 141578 • Austin, TX 78714

STATE OF NH
DEPT OF JUSTICE
2017 MAR -3 AM 11:57

00001
ACD1234
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

February 24, 2017

RE: Notice of Data Breach

Dear John Sample:

I am writing regarding a recent incident that may affect the security of certain personal information related to you. I wanted to provide you with information about this incident, my response and steps you can take to protect against identity theft and fraud, should you feel it necessary to do so.

What Happened? On the morning of February 10, 2017 I discovered that my car had been stolen sometime between the night of February 9, 2017 and that morning. I quickly reported this incident to law enforcement and have been cooperating with their investigation. Inside my trunk were two password protected laptop computers containing tax software for my personal tax clients. That software contained personal tax information including the Social Security numbers and birthdates for all of the persons listed on your tax return (spouse and dependents). If you ever provided me bank accounts used for Direct Deposit, then you should alert your banking institution for that particular account and follow their advice. One of the laptops possibly included tax years as far back as 2010. I have no evidence that the laptops were targeted or that the information stored on the laptops at the time they were stolen was accessed or acquired by an unauthorized individual.

What Information Was Involved? The stolen laptops stored certain data related to you, including a combination of name, address, date of birth, Social Security number, and bank account information. There may also be information related to a spouse or dependents if provided for previous tax filings. I will be notifying all impacted individuals separately, so if your spouse or dependent is impacted, they will be sent a letter.

What I Am Doing. I have also been working to notify those who may be impacted and provide them with resources to assist them in protecting against any possible identity theft or fraud.

As an added precaution, I have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-725-5772 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-725-5772 using the following redemption code: Redemption Code

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do. You can enroll in the monitoring service using the enrollment information above. You can also review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud" which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

For More Information. I sincerely regret any inconvenience or concern this incident has caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at 1-855-725-5772. The call center is available Monday through Saturday, 6:00 a.m. to 6:00 p.m. P.S.T. (excluding U.S. holidays).

Sincerely,

John Williamson, CPA

Steps You Can Take to Protect Against Identity Theft and Fraud

You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies. California filers can visit The State of California Franchise Tax Board's website regarding how to report scams, identity theft, and tax fraud at https://www.ftb.ca.gov/online/fraud_referral/index.shtml.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain new credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.