ARCHER
ATTORNEYS AT LAW

Robert T. Egan

regan@archerlaw.com
856-354-3079 Direct
856-673-7079 Direct Fax

Archer & Greiner, P.C.
One Centennial Square
Haddonfield, NJ 08033
856-795-2121 Main
856-795-0574 Fax
www.archerlaw.com

April 19, 2018

VIA UPS

Office Of The Attorney General
Consumer Protection And Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

RE: NOTICE OF DATA BREACH - LI Tax and Planning, Inc.

Dear Attorney General Foster:

Our client, LI Tax and Planning, Inc. ("LI Tax"), understands the importance of protecting personal information provided by its customers and therefore provides this notice to your office pursuant to N.H. Rev. Stat. Ann. §359-C:20. By providing this notice, LI Tax does not waive any defenses which may be available to it and does not otherwise consent to personal jurisdiction in New Hampshire.

LI Tax is a recently-formed New York corporation that purchased the assets (but not the liabilities) of an existing tax preparation company, LI Tax78, Inc., d/b/a LI Tax and Financial Services ("LIT78"), with an office in West Babylon, New York, on February 1, 2018. LI Tax subsequently learned of breaches of the computer systems of LIT78 that had occurred before February 1, 2018, but which had not been disclosed to LI Tax prior to the asset acquisition.

LI Tax did not learn of the breaches until February 25, 2018 - after the tax season began - after it hired an independent third-party forensic team to investigate why several customers' tax returns had been rejected by the Internal Revenue Service ("IRS"). That forensic team determined that, on or about November 1, 2017, an unauthorized individual gained access to LIT78's computer system and exfiltrated a data file containing clients' personally identifiable information to a unfamiliar cloud service, Mega.nz. The file taken included certain LIT78 clients' full names, addresses, and social security numbers (SSN) along with their wage and other tax-related information. It also included many clients' telephone numbers, email addresses, and occupations. LI Tax's investigation indicates that four (4) New Hampshire residents' information was exfiltrated.

It is possible that other personal information, including that regarding other tax years and information relating to other clients of LIT78, was also taken from the LIT78's computer system at approximately the same time, but LI Tax does not have any digital evidence that proves that it

was. LI Tax's investigation indicates that LIT78 did not have any clients who were residents of New Hampshire other than the four (4) New Hampshire residents whose information was exfiltrated.

In addition, on three separate occasions during the LIT78's ownership (in August 2017 and January 2018), its computer systems were breached by unknown actors and inflicted with ransomware, which blocked access to certain data files. It is possible that the ransomware attacks blocked access to data files on the LIT78's computer system that may have included clients' personal information. However, LI Tax has no evidence that shows that any of these data files or the information in them were taken.

In response, despite the fact that these breaches occurred before LI Tax acquired the assets of LIT78, LI Tax has mailed written notification to the four (4) New Hampshire residents in accordance with N.H. Rev. Stat. Ann. §359-C:20, in the form of the documents enclosed herewith. Additionally, LI Tax has alerted the IRS and the local New York authorities about the data breach. LI Tax has retained Kroll Information Assurance, LLC ("Kroll") through which it is offering each of the four (4) residents one-year of free credit monitoring and $1,000,000 in identity theft insurance and has set up a dedicated call center that potentially affected individuals can call with questions regarding the incident.

LI Tax is continuing to work closely with reputable security experts to identify and implement measures to further strengthen the security of its system to help prevent data breaches from happening in the future. It has migrated clients' data from LIT78's computer system onto a new, more secure system and implemented controls on data access using the latest security protocols recommended for our industry. It employs an external technology firm to manage security and keep it current with all anti-virus, malware, and cybersecurity defenses. It is also in the process of reinforcing its information security training program with an emphasis on the detection and avoidance of similar scams.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

ROBERT T. EGAN

RTE:jlv
cc: LI Tax and Planning, Inc.
214293250v1

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>> <<State>> <<ZipCode>>

NOTICE OF DATA BREACH

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

LI Tax and Planning, Inc. ("LI Tax") values the relationship we have with our customers and understands the importance of their information. We are writing because of a cyber incident that might have resulted in the disclosure of your personal information. LI Tax and its management team are taking an aggressive approach to this incident in order to help customers protect against potential fraud.

What Happened

On February 1, 2018, our company, LI Tax, purchased the assets of your previous tax preparer, LI Tax78, Inc., that did business as "LI Tax and Financial Services". Unknown to us, before we acquired the assets, a scammer had accessed the old company's computer system and stolen a data file containing personal information regarding clients for whom the old company had prepared 2016 taxes. Your personal information was not included in that file. However, it is possible that other personal information, including information regarding other tax years and information regarding other clients, was also stolen from the old company's computer system at approximately the same time. This theft was not disclosed to us before we acquired the assets of the business from the previous owner.

In addition, on three separate occasions during the old company's ownership (in August 2017 and January 2018), its computer systems were breached by unknown actors and inflicted with ransomware - a type of malicious software designed to block access to a computer system or data on a computer system until a sum of money is paid. The ransomware software blocked access to certain data files on the old company's computer system. This ransomware activity was not disclosed to us before our company acquired the assets of the business from the previous owner.

We learned of these breaches on February 25, 2018 – after the tax season began - when it was discovered by a third-party digital forensic team whom we retained to investigate unrelated irregularities in the computer system that we bought from the old company.

What Information Was Involved

We have determined that it is **possible** that your personal information was taken (or "exfiltrated") by scammers from the old company's computer system without authorization before LI Tax acquired the assets, **although we do not have any evidence that proves that it was**. This might have included your full name, address, and Social Security number (SSN), wage and other tax-related information, telephone number, email address, and occupation.

In addition, it is possible that the ransomware attacks blocked access to other data files on the old company's computer system that may have included your personal information. **However, we have no evidence that shows that any of these other data files or the information in them were taken.**

What We've Done

Immediately following the discovery of the data breach, we contacted a number of professionals to work through what we feel was the best plan to protect you from fraud. We also contacted our local authorities, state authorities, and the Internal Revenue Service in order to try and stop any fraud before it may begin.

We also migrated your data from the old company's computer system onto a new, more secure system and implemented controls on data access using the latest security protocols recommended for our industry. We employ an external technology firm to manage our security and keep us current with all anti-virus, malware, and cybersecurity. We take security very seriously and have taken all necessary steps to prevent incidents from happening in the future. We are also in the process of reinforcing our information security training program with an emphasis on the detection and avoidance of similar scams.

Despite the fact that your information was stolen from the old company's computer systems before LI Tax acquired its assets, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

This is completely free to you and activating these services should not impact your credit score. **We encourage you to activate as soon as possible.** However, in order to get these benefits, you must activate the monitoring – **we cannot do it for you**.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
*You have until **July 19, 2018** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-219-9085. Additional information describing your services is included with this letter.

What You Can Do

Because we value your security, we are taking this action to notify you following our investigation so that you can take appropriate steps to protect yourself. Additionally, as noted above, LI Tax is offering every potentially affected individual one year of identity monitoring for free.

Finally, we have included an "Additional Resources" section with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

One way scammers use W-2 information is by filing fraudulent tax returns in order to get tax refunds. We recommend that you contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 to enable the IRS to try to monitor your account this year, but given the unfortunately large volume of these kinds of scams, they may not be successful in catching all fraudulent activity. For this reason, we recommend that you file your income tax returns as early as possible to help prevent any fraudulent returns from being filed on your behalf. If a fraudulent tax return is filed, you will still likely be entitled to receive any refund that you are owed, but it will take some time to work through the process of correcting your tax return with the IRS and state taxing authorities. You will find additional information about tax returns at https://www.irs.gov/individuals/data-breach-information-for-taxpayers.

For More Information

We apologize for any inconvenience or concern this may have caused. If you have any questions regarding your services, please call 1-833-219-9085, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your Membership Number ready.

Alternatively, you may contact me at:

LI Tax and Planning, Inc.
470 Sunrise Highway
West Babylon, NY 11704
breach@longislandtax.net

Sincerely,

Elizabeth Boonin
President

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

1. **Review your credit reports.** Even if you choose not to take advantage of the free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. To obtain the free reports, you can: Call 1-877-322-8228; Order online at www.annualcreditreport.com; or Complete the Annual Credit Report Request Form, available at www.ftc.gov/credit, and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111	Phone: 1-888-397-3742	Phone: 1-888-909-8872
P.O. Box 740256	P.O. Box 2104	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Atlanta, GA 30348-5281
www.equifax.com	www.experian.com	www.transunion.com

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s). If you discover any suspicious items, notify your card issuing bank immediately. In the unlikely event that you fall victim to identity theft as a consequence of this incident, they will work on your behalf to identify, stop and reverse the damage quickly. You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. **Security Freeze.** You can place a security freeze on your credit report. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

   To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Trans Union Security Freeze	Equifax Security Freeze	Experian Security Freeze
Fraud Victim Assistance Department	P.O. Box 105788	P.O. Box 9554
P.O. Box 2000	Atlanta, GA 30348	Allen, TX 75013
Chester, PA 19022-2000	www.equifax.com	www.experian.com
www.transunion.com	Phone: 1-800-349-9960	Phone: 1-888-397-3742
Phone: 1-888-909-8872		

   In order to request a security freeze, you will need to provide the following information:

   1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
   2. Social Security Number;
   3. Date of birth;
   4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
   5. Proof of current address such as a current utility bill or telephone bill;
   6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

3. **Tax-Related Identity Theft.** If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps: Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov. Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions. Continue to pay your taxes and file your tax return, even if you must do so by paper. If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.

4. **Place Fraud Alerts with the three credit bureaus.** Because your Social Security number was involved, you may also want to place a fraud alert on your credit file. An initial fraud alert lasts 90 days and tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit reporting companies. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three bureaus will send you your credit report to review, free of charge.

   To place a fraud alert on your credit report, contact one of the credit reporting companies (you do not need to contact all of them):

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

   Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

   All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338). **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft. **Illinois Residents:** Illinois Attorney General, Consumer Fraud Bureau, 500 South Second Street, Springfield, IL 62701, Telephone: 217-782-1090 or 1-800-243-0618 (toll free in IL). **New York Residents:** For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website

at www.dos.ny.gov/consumerprotection. **Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or http://www.oag.state.md.us. **Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **North Carolina Residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; or http://www.ncdoj.gov. **IF YOU ARE A RESIDENT OF ANY OTHER STATES:** Your state Attorney General's Office and website may provide relevant information.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.

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

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

NOTICE OF DATA BREACH

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

We are writing to tell you about a data security incident that may have exposed some of your personal information. LI Tax and Planning, Inc. ("LI Tax") values the relationship we have with our customers and understands the importance of their information. We are writing because of a cyber incident that resulted in the disclosure of your personal information. LI Tax and its management team are taking an aggressive approach to this incident in order to help customers protect against potential fraud.

What Happened

On February 1, 2018, our company, LI Tax, purchased the assets of your previous tax preparer, LI Tax78, Inc., that did business as "LI Tax and Financial Services". Unknown to us, before we acquired the assets, a scammer had accessed the old company's computer system and stolen a data file containing personal information regarding your 2016 taxes. It is possible that other personal information, including that regarding other tax years, was also stolen from the old company's computer system at approximately the same time. This theft was not disclosed to us before we acquired the assets of the business from the previous owner.

In addition, on three separate occasions during the old company's ownership (in August 2017 and January 2018), its computer systems were breached by unknown actors and inflicted with ransomware - a type of malicious software designed to block access to a computer system or data on a computer system until a sum of money is paid. The ransomware software blocked access to certain data files on the old company's computer system. This ransomware activity was not disclosed to us before our company acquired the assets of the business from the previous owner.

We learned of these breaches on February 25, 2018 – after the tax season began - when it was discovered by a third-party digital forensic team whom we retained to investigate unrelated irregularities in the computer system that we bought from the old company.

What Information Was Involved

We have determined that various information regarding your 2016 taxes was taken (or "exfiltrated") by scammers from the old company's computer system without authorization before LI Tax acquired the assets. This included your full name, address, and Social Security number (SSN) along with your wage and other tax-related information. It may have included your telephone number, email address, and occupation. It is possible that other personal information, including that regarding other tax years, was also taken, but we do not have any concrete evidence that proves that it was.

In addition, it is possible that the ransomware attacks blocked access to other data files on the old company's computer system that may have included your personal information. **However, we have no evidence that shows that any of these other data files or the information in them were taken.**

What We've Done

Immediately following the discovery of the data breach, we contacted a number of professionals to work through what we feel was the best plan to protect you from fraud. We also contacted our local authorities, state authorities, and the Internal Revenue Service in order to try and stop any fraud before it may begin.

We also migrated your data from the old company's computer system onto a new, more secure system and implemented controls on data access using the latest security protocols recommended for our industry. We employ an external technology firm to manage our security and keep us current with all anti-virus, malware, and cybersecurity. We take security very seriously and have taken all necessary steps to prevent incidents from happening in the future. We are also in the process of reinforcing our information security training program with an emphasis on the detection and avoidance of similar scams.

Despite the fact that your information was stolen from the old company's computer systems before LI Tax acquired its assets, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

This is completely free to you and activating these services should not impact your credit score. **We encourage you to activate as soon as possible.** However, in order to get these benefits, you must activate the monitoring – **we cannot do it for you**.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **July 19, 2018** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-219-9085. Additional information describing your services is included with this letter.

What You Can Do

Because we value your security, we are taking this action to notify you following our investigation so that you can take appropriate steps to protect yourself. Additionally, as noted above, LI Tax is offering every affected individual one year of identity monitoring for free.

Finally, we have included an "Additional Resources" section with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

One way scammers use W-2 information is by filing fraudulent tax returns in order to get tax refunds. We recommend that you contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 to enable the IRS to try to monitor your account this year, but given the unfortunately large volume of these kinds of scams, they may not be successful in catching all fraudulent activity. For this reason, we recommend that you file your income tax returns as early as possible to help prevent any fraudulent returns from being filed on your behalf. If a fraudulent tax return is filed, you will still likely be entitled to receive any refund that you are owed, but it will take some time to work through the process of correcting your tax return with the IRS and state taxing authorities. You will find additional information about tax returns at https://www.irs.gov/individuals/data-breach-information-for-taxpayers.

For More Information

We apologize for any inconvenience or concern this may have caused. If you have any questions regarding your services, please call 1-833-219-9085, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your Membership Number ready.

Alternatively, you may contact me at:

LI Tax and Planning, Inc.
470 Sunrise Highway
West Babylon, NY 11704
breach@longislandtax.net

Sincerely,

Elizabeth Boonin
President

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

1. **Review your credit reports.** Even if you choose not to take advantage of the free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. To obtain the free reports, you can: Call 1-877-322-8228; Order online at www.annualcreditreport.com; or Complete the Annual Credit Report Request Form, available at www.ftc.gov/credit, and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111	Phone: 1-888-397-3742	Phone: 1-888-909-8872
P.O. Box 740256	P.O. Box 2104	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Atlanta, GA 30348-5281
www.equifax.com	www.experian.com	www.transunion.com

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s). If you discover any suspicious items, notify your card issuing bank immediately. In the unlikely event that you fall victim to identity theft as a consequence of this incident, they will work on your behalf to identify, stop and reverse the damage quickly. You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. **Security Freeze.** You can place a security freeze on your credit report. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

   To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Trans Union Security Freeze	Equifax Security Freeze	Experian Security Freeze
Fraud Victim Assistance Department	P.O. Box 105788	P.O. Box 9554
P.O. Box 2000	Atlanta, GA 30348	Allen, TX 75013
Chester, PA 19022-2000	www.equifax.com	www.experian.com
www.transunion.com	Phone: 1-800-349-9960	Phone: 1-888-397-3742
Phone: 1-888-909-8872		

   In order to request a security freeze, you will need to provide the following information:

   1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
   2. Social Security Number;
   3. Date of birth;
   4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
   5. Proof of current address such as a current utility bill or telephone bill;
   6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

3. **Tax-Related Identity Theft.** If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps: Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov. Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions. Continue to pay your taxes and file your tax return, even if you must do so by paper. If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.
4. **Place Fraud Alerts with the three credit bureaus.** Because your Social Security number was involved, you may also want to place a fraud alert on your credit file. An initial fraud alert lasts 90 days and tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit reporting companies. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three bureaus will send you your credit report to review, free of charge.

   To place a fraud alert on your credit report, contact one of the credit reporting companies (you do not need to contact all of them):

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

   Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

   All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338). **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft. **Illinois Residents:** Illinois Attorney General, Consumer Fraud Bureau, 500 South Second Street, Springfield, IL 62701, Telephone: 217-782-1090 or 1-800-243-0618 (toll free in IL). **New York Residents:** For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website

at www.dos.ny.gov/consumerprotection. **Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or http://www.oag.state.md.us. **Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **North Carolina Residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; or http://www.ncdoj.gov. **IF YOU ARE A RESIDENT OF ANY OTHER STATES:** Your state Attorney General's Office and website may provide relevant information.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.