JOHN N. FERNÉZ
CERTIFIED PUBLIC ACCOUNTANT
11 South Main Street, Suite 4
Marlborough, CT 06447
860-295-0729
jfernezcpa@snet.net

[INSERT NAME]
[INSERT ADDRESS]
[INSERT CITY, STATE, ZIP]

June 13, 2025

RE: Notice of Data Breach

Dear [INSERT NAME],

In follow up to our telephone conversation, I am writing to you with important information about a breach of security involving your personal information caused by a compromise of the Intuit cloud-based tax software account used by John N. Fernez CPA, LLC.

What Happened and Our Response
On April 16, 2025, I was notified by Intuit, the provider of the cloud-based tax software we use to process and electronically file tax returns, that certain tax filings were submitted to the IRS without my permission. My investigation with Intuit revealed that an unauthorized individual (the "threat actor") had signed into my account and filed fraudulent tax returns.

Upon discovery, I took immediate action to change my account password with Intuit and began the process of contacting each of my clients by telephone to inform them of the situation. On April 16, 2025 I notified the Internal Revenue Service (IRS) of the breach and filing of fraudulent tax returns and deactivated my Electronic Filer Identification Number (EFIN).

What Information Was Involved
You are receiving this notice because the data compromised by the threat actor contained information about you including your name, address, telephone number, email address, social security number, financial information, and tax return data. Certain bank account numbers included among your tax return data may have also been compromised, however, no access codes, PINs, or other data that could be used to gain access to those accounts were included.

For your protection, we are offering you credit monitoring and fraud assistance services at no cost to you for two years. Please refer to the information below and attached to this notice for details about how to activate these services.

What are We Doing to Mitigate Future Risks

As discussed above, upon learning of the compromise of the Intuit account, I immediately changed my login password to prevent further access by the threat actor. I have had an IT professional perform a deep scan of all of our devices for malware and viruses; none were found. Also, all passwords related to any financial and tax applications have been changed.

What You Can Do

In addition to the measures we discussed with respect to resolving the fraudulently filed tax return with the IRS, I encourage you to monitor your financial statements and activity closely and report any suspicious transactions to your financial institution(s) and law enforcement. I also recommend that you activate the credit monitoring services being offered as soon as possible. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the credit bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. For more information on these services available from TransUnion, including instructions on how to activate your complimentary twenty-four (24) months membership, please see the additional information within Attachment 1 to this letter. Additionally, we have included some further helpful information about how to generally protect yourself within Attachment 2.

For More Information

The Reference Guide (Attachment 2) provides some helpful information about protecting your identity. If you would like additional information or wish to speak with me, you may contact me at 860.295.0729 during normal business hours or via email at jfernezcpa@snet.net.

We take our responsibility to safeguard your personal information very seriously. Unfortunately, businesses that process data on behalf of individuals continue to be targeted for data theft and fraud. We will continue to evaluate and enhance our security measures on a regular basis. I regret the occurrence of this incident and sincerely apologize that your personal information was compromised in connection with it.

Respectfully,

John N. Fernez CPA

Attachment 1: Credit Monitoring / Fraud Assistance Services

How do I enroll for the free services?

24 Months of service

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: **<INSERT CODE HERE>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires 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.

Attachment 2: Identity Protection Reference Guide

The following are recommended steps for generally protecting yourself from identity theft or other misuse of your personally identifiable information:

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.
Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.
When you receive your credit report, review it carefully. Look for accounts you did not open and medical bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.
If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

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

Place a Fraud Alert on Your Credit File. If you choose not to enroll for the TransUnion services being offered, you may place a fraud alert on your own. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below.

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

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
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 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.
- Be sure to promptly report any suspicious activity to John N Fernez CPA, LLC and to law enforcement.

Additional information for residents of the following states:
Connecticut: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, http://www.ct.gov/ag

New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in regard to this 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.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. There is no longer a fee for placing, lifting, and/or removing a security freeze.

Information about placing a security freeze on your credit report:
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:

- Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348
- Experian Security Freeze P.O. Box 9554 Allen, TX 75013
- Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

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.)

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.