



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

[REDACTED]

Postal Endorsement Line

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Accounting & Tax Associates, Inc (“Accounting & Tax”). We are writing with important information regarding a data security incident that may have involved some of your personal information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

On or around May 14, 2025, an unauthorized party accessed Accounting & Tax’s account on the third-party account software, Intuit Inc. Lacerte Tax (“Lacerte Tax”). Upon learning of this issue, we promptly launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine whether any sensitive data had been compromised. After our extensive review concluded on July 2, 2025, we determined that your personal information may have been included within the data that was impacted by the incident, including your name and [REDACTED]

Out of an abundance of caution to protect you from potential misuse of your information, we are offering a complimentary 18-month membership for credit monitoring. For more information on identity theft prevention and credit monitoring, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your information.

If you have any further questions regarding this incident, please call the dedicated, confidential toll-free response line we have set up to respond to questions at 833-594-5310. The response line is available Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern time, excluding holidays.

Sincerely,

Accounting & Tax Associates, Inc
264 North Main Street
Suite 3
East Longmeadow, MA 01028

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.

Accounting & Tax has retained **NortonLifeLock** to provide 18-months of complimentary **LifeLock Ultimate Plus™** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **www.LifeLock.com**. Click on the yellow “**START MEMBERSHIP**” button (*do not attempt registration from a link presented by a search engine*).
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code:** [REDACTED] and click the “**APPLY**” button.
3. On the next screen, enter your **Member ID:** [REDACTED] and click the “**APPLY**” button.
4. Your complimentary offer is presented. Click the red “**START YOUR MEMBERSHIP**” button.
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL instructions in this email*).

Alternatively, to activate your membership over the phone, please call: 1-800-899-0180

You will have until October 31, 2025 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Ultimate Plus™** membership includes:

- ✓ LifeLock Identity Alert™ System[†]
- ✓ Dark Web Monitoring^{**}
- ✓ LifeLock Privacy Monitor™
- ✓ USPS Address Change Verification
- ✓ Lost Wallet Protection
- ✓ Reduced Pre-Approved Credit Card Offers
- ✓ Fictitious Identity Monitoring
- ✓ Court Records Scanning
- ✓ Data Breach Notifications
- ✓ Credit, Checking and Savings Account Activity Alerts^{†**}
- ✓ Checking and Savings Account Application Alerts^{†**}
- ✓ Bank Account Takeover Alerts^{†**}
- ✓ Investment Account Activity Alerts^{†**}
- ✓ Three-Bureau Credit Monitoring^{†**}
- ✓ Three-Bureau Annual Credit Reports & Credit Scores^{†**}

The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

- ✓ File-Sharing Network Searches
- ✓ Sex Offender Registry Reports
- ✓ Priority 24/7 Live Member Support
- ✓ U.S.-based Identity Restoration Specialists
- ✓ Stolen Funds Reimbursement up to \$1 million^{†††}
- ✓ Personal Expense Compensation up to \$1 million^{†††}
- ✓ Coverage for Lawyers and Experts up to \$1 million^{†††}

[†]If your plan includes credit reports, scores, and/or credit monitoring features (“Credit Features”), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. [†] LifeLock does not monitor all transactions at all businesses.

^{**}These features are not enabled upon enrollment. Member must take action to get their protection.

^{†††} Reimbursement and Expense Compensation, each with limits of up to \$1 million for Ultimate Plus. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, contact any one of the three (3) major credit bureaus at the numbers or addresses listed below. As soon as one (1) credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three (3) nationwide credit-reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, then you may file a police report in the City in which you currently reside.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

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. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

6. Reporting Identity Fraud to the IRS.

If your attempt to file your federal tax return electronically was rejected, or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- **File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>)**
 - *Instructions for Form 14039* – In Section A check box 1. / In Section B check box 2. / Insert this in the “Please provide an explanation” box: I receive notice that my name and Social Security number may have been used to file a fraudulent tax return that was accepted by the IRS and/or state tax agency.
 - This form should be mailed or faxed to the IRS: Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
- Call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and/or
- File a police report with your local police department. It may be appropriate to provide a copy of this letter.

Additional information regarding preventing tax-related identity theft can be found at: <http://www.irs.gov/uac/Identity-Protection>.

For further information and guidance from the IRS about tax-related identity theft, please visit: <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft> (Taxpayer Guide to Identity Theft) and <https://www.irs.gov/pub/irs-pdf/p5027.pdf> (IRS Publication 5027, Identity Theft Information for Taxpayers).

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.