



**DOUGLAS M. SMITH
& COMPANY**

CERTIFIED PUBLIC ACCOUNTANTS

2767 EAST SHAW AVENUE, SUITE #102, FRESNO, CALIFORNIA 93710

TEL. (559) 294-6592 · FAX (559) 294-6593

DATE, 2020

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

RE: Important Notice of Data Incident. Please read this entire letter.

Dear [Insert name]:

We are contacting you to report that your electronically filed tax return was rejected by our company's tax preparation software, Lacerte by Intuit, and that Lacerte has informed us that a fraudulent return has already been filed under your name. As such, it appears that your Social Security Number has been compromised, which is necessary to file any return with the IRS.

We have engaged forensic investigators to analyze our servers, and our initial investigation has found no evidence that any unauthorized access or compromise of our computer systems, where your personal information is stored. We have also confirmed that no virus or malicious software has been installed on our computer network. Even so, as a protection to you, we are providing this notification and one year of complimentary credit monitoring. Enrollment instructions are provided below under "Credit Monitoring."

WHAT HAPPENED

Between March 25, 2020 and April 1, 2020, 32 electronically filed tax returns were rejected by the Lacerte software, including yours, which Lacerte reported was due to the fact a return in your name had apparently already been filed. We immediately retained forensic investigators and legal counsel to conduct an investigation, and, to date, we have found no evidence that any unauthorized individual has accessed our systems. We have confirmed no malicious software is present on our systems, and there is no evidence of any firewall or network compromise. Even so, as our investigation continues, we are providing this notice along with complimentary credit monitoring and fraud protection to minimize any possible risk of identity theft.

WHAT INFORMATION IS INVOLVED

Your Social Security Number was required to file the fraudulent tax return, and, as such, we know that it has been compromised at some point in time. Public information, including name, address and date of birth, may have also been used to file the return.

WHAT WE ARE DOING

While we have identified no evidence of any compromise of our computer systems, our forensic investigation into this incident is continuing. We have also taken appropriate security measures, including global password changes, ongoing malware scans and network monitoring.

We are also working with the IRS and Lacerte to resolve any issues regarding the fraudulent returns, and to ensure that the correct return is filed, and the full refund is paid to you, as swiftly as possible.

CREDIT MONITORING

We are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Public Records monitoring/Cyber 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. Also, the following public records will

be monitored: Change of Address, Court Records and Social Security number trace, Payday Loan and Sex Offender. The cyber monitoring will review the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by CyberScout, a company that specializes in identity theft education and resolution.

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: **<CODE HERE.>**

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

You are encouraged to remain vigilant against identity theft, including over the next twelve to twenty-four months, by regularly reviewing financial account statements and monitoring credit reports for suspicious activity, and to immediately report any unauthorized charges to the card issuer. The phone number to call is usually on the back of the credit or debit card. Any incidents of suspected identity theft may be reported to financial institutions and law enforcement. 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.

You also have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who may access the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies:

Equifax

P.O. Box 10569
Atlanta, Georgia 30348
1-866-836-3651 / 1-800-525-6285
www.equifax.com

Experian

P.O. Box 4500
Allen, Texas 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, Pennsylvania 19106
1-800-916-8800 / 1-800-680-7289
www.transunion.com

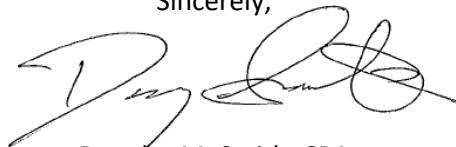
As an alternative to a security freeze, you have the right to place a "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies. You may also contact the Federal Trade Commission for additional information regarding consumer protection at:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Ave., NW
Washington, DC 20580

Toll-Free: (877) 438-4338
TTY: 1-866-653-4261
<https://www.identitytheft.gov>

In closing, we recommend that you enroll in the complimentary credit monitoring using the instructions referenced above, which service is at no cost to you. Should you have any questions or concerns regarding this matter, please do not hesitate to contact Douglas Smith at 559-294-6592.

Sincerely,



Douglas M. Smith, CPA

* 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.