



**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 as a dependent of a client of Douglas M. Smith & Company, CPAs, to report that between March 31 and April 1, 2020, four (4) tax returns electronically filed by our firm were rejected, apparently because fraudulent returns had already been filed for those taxpayers.

Your information was NOT included on any rejected return, and there is no evidence of any suspicious activity relating to your personal information, including Social Security Number; however, as required by law, we are providing this notification to all our clients and dependents. We are also providing one year of complimentary credit monitoring, fraud monitoring, and \$1,000,000 in Identity Theft Insurance for all clients and their dependents in an abundance of caution. Enrollment instructions are provided below under "Credit Monitoring."

We are working with the IRS and Secret Service to ensure that every client receives a full refund, including those identified on any fraudulent returns, and we have directed the IRS to "flag" your account to prevent anyone other than our office from filing a return on your behalf. Rest assured, no client needs to worry about losing their refund.

WHAT HAPPENED

Between March 31, 2020 and April 1, 2020, four (4) electronically filed tax returns were rejected by the Intuit Lacerte tax preparation software, which Lacerte reported was due to the fact that returns were previously filed for those taxpayers. We immediately reported this incident to the IRS, Secret Service, Fresno Police and FBI, and, working with Lacerte, identified a total of 30 fraudulent returns. You are **not** among the individuals identified on the 30 fraudulent returns.

We also immediately retained forensic investigators to conduct an investigation, and, to date, we have found no evidence that any unauthorized individual has accessed our computer systems, where your personal information is stored.

WHAT INFORMATION IS INVOLVED

To the best of our knowledge, there has been no suspicious activity with respect to you or any other clients and dependents who were not identified on the 30 impacted returns. For the 30 fraudulent returns, the taxpayer's Social Security Number, along with public information including name, address and date of birth, was used to file the return. **You are not impacted by the 30 fraudulent returns,** but, your Social Security Number is stored on our server as the dependent of our client, which is why we are legally required to provide this notification.

WHAT WE ARE DOING

We immediately notified the IRS of the 30 impacted returns, and directed the IRS to "flag" you and all other clients and dependents to prevent anyone other than our office from filing returns using your information. We also retained forensic investigators to analyze our computer systems and information, and hired a new IT and cybersecurity firm to manage all security going forward. And, we are providing one year of credit monitoring, fraud monitoring, and \$1,000,000 in Identity Theft Insurance for all clients and dependents in an abundance of caution to minimize risk of identity theft.

CREDIT MONITORING

We are providing you with one year of 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>

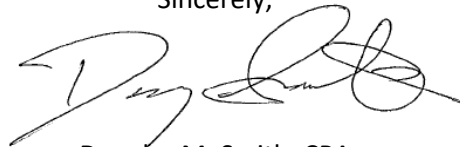
In closing, we believe we are taking every possible step to protect you following this incident. To the best of our knowledge, there has been no suspicious activity regarding your personal information, and we have found no evidence that any unauthorized individual accessed our computer systems.

No client will need to worry about losing their refund, as we continue to work with the IRS and Secret Service regarding the 30 impacted returns, and have directed the IRS to “flag” your account to prevent any fraudulent filings using your personal information.

We recommend that you enroll in the complimentary credit monitoring, fraud monitoring, and \$1,000,000 in Identity Theft Insurance using the instructions referenced above, which service is at no cost to you. If you believe there is any possibility that someone is using your personal information, you can contact a CyberScout personal advocate [HOW??] to work with you in reporting the problem and helping you through the entire identity restoration process.

We thank you for your understanding, and if you have any questions or concerns regarding this matter, please do not hesitate to contact me at 559-294-6592.

Sincerely,

A handwritten signature in black ink, appearing to read 'Douglas M. Smith', with a stylized flourish at the end.

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.