Taylor Bethell, CPA
<Return Address>
<City> <State> <Zip>

Date

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><PostalCode+4>

NOTICE OF DATA BREACH

Dear <FirstName> <LastName>,

Please read this letter in its entirety.

We are writing to provide you with a formal notification regarding a data incident that occurred at RF Associates, LLC, in which your information may have been accessed by an unauthorized user. This letter serves to provide additional information concerning the incident, what is being done to correct it, and what you can do to further protect your information.

What Happened?

On _____, we discovered that an unauthorized user had gained access to our network and attempted to file a fraudulent tax return on your behalf. Fortunately, the IRS has advised that the fraudulent tax return was rejected. We believe this occurred on or around February 20, 2025. We are providing you with notice so that you may be proactive in protecting your data.

We immediately began an investigation with the assistance of IT specialists to determine the full nature and scope of this incident. The investigation is ongoing; however, we are confident that a threat actor has accessed your sensitive data in our third party tax filing software, Lacerte. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected.

Beyond filing a fraudulent tax return on your behalf, we have no information that your sensitive data has been misused in any other manner by the threat actor. That said, we are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have. If we become aware of any suspicious activity in connection with your tax returns, we will notify you immediately. Conversely, if you receive any notifications from the IRS concerning suspicious activity on your account, please notify our office right away.

What Information Was Involved?

While our investigation has not revealed the precise information which may have been accessed by the threat actor, the information could have included any information that is part of your tax return files, such as social security numbers, names, driver's license numbers, bank account information, and/or other sensitive information you may have also provided to us.

What We Are Doing.

In response to this incident, we implemented additional security measures to further protect our network and reduce the risk of a similar incident occurring in the future.

Further, we are working with the appropriate agencies on your behalf. The FBI and Secret Service have been notified of this incident. This notification to you was not delayed as a result of law enforcement investigation.

Additionally, we have notified the IRS and our EFIN has been changed for heightened security on tax filings going forward.

We are currently conducting a forensic review of the network to determine the scope of the breach. If we learn that your sensitive information has been compromised beyond that which is available in Lacerte, we will let you know immediately.

Further, we are committed to providing you with Credit Monitoring Services. These services will be provided by Cyberscout, a TransUnion company, at no cost to you for the next 18 months. To take advantage of these services, 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: <<**Unique Code**>>. 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.

Commented [FR1]: Credit monitoring services

We are taking this matter very seriously and are committed to helping those people who may have been impacted by this unfortunate situation.

What You Can Do.

Additionally, if you have not done so already, you should do the following:

If you choose not to enroll in the Credit Monitoring services being offered by our office above, you can obtain Credit Monitoring by contacting one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

- Obtain free copies of your credit report and monitor them upon receipt for any suspicious activity.
- Be sure to promptly report any suspicious activity to Taylor Bethell, CPA.

- We strongly recommend you be vigilant in reviewing your bank accounts and other financial account statements, as well as monitoring your Credit Monitoring or free credit reports.
    - If you should like to request a free security freeze from these agencies, you will need the following information: (1) proof of your identity, typically your Social Security

Card; (2) proof of your address in two forms, such as on your driver's license, utility bill, bank statement, etc.; (3) your date of birth; and (4) contact information.

- You have the right to obtain a police report.
- If you suspect fraudulent activity, report it to law enforcement, including the Federal Trade Commission at https://www.identitytheft.gov/#/ and your State Attorney General's Office at https://www.naag.org/find-my-ag/.
- You can obtain more information from the Federal Trade Commission and your State Attorney General's Office about identity theft, fraud alerts, security freezes, and the protection of your sensitive information. The Federal Trade Commission can be contacted as follows:

  - **Federal Trade Commission**
    600 Pennsylvania Avenue, NW
    Washington, DC 20580
    1-877-382-4357
    https://www.consumer.ftc.gov/

For More Information.

We are committed to helping those people who may have been impacted by this unfortunate situation. Protecting your information is incredibly important to us, as is addressing this incident with the information and assistance you may need. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact Taylor Bethell at tbethell@rfacpas.com or at (503) 244-7016.

Cyberscout representatives are available for 90 days from <<Date>>, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

Commented [FR2]: Please make sure to letting know when will be sent the letters since we sent the codes from 5/6/25 please not longer from May 16 since our codes also will have 90 days actives, I requested few more days (until August 16th).

Commented [FR3R2]: Call Center info

Sincerely,

Taylor Bethell