Daniel E. Fitzgerald, CPA
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08411 1-1

Daniel E. Fitzgerald
Certified Public Accountant
2909 Coffee Road, Suite 11 · Modesto, CA 95355 · 209.576.0761 · FAX 209.576.0637

[redacted]

May 14, 2024

NOTICE OF DATA BREACH

Dear [redacted]:

Please read this letter in its entirety.

I am writing to provide you with a formal notification regarding a data incident involving Daniel E. Fitzgerald, CPA's computer system, in which your personal information may have been accessed. This letter serves to provide additional information concerning the incident, what has been done to correct it, and what you can do to further protect your information.

What Happened?
On January 11, 2024, our office discovered that our office had fallen victim to a ransomware attack and the threat actor had gained unauthorized access to our computer network. Upon learning this information, we immediately worked with our IT consultants to investigate the breach, take the affected systems offline, and to institute corrective measures to prevent further unauthorized access to our network. Within 48 hours of discovering the breach, we restored our network using a backup system located offsite.

We have no information that your sensitive data has been accessed or misused in any manner by the threat actor, or that your tax returns have been impacted in any way. 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 further 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?
For Individuals: While our investigation has not revealed the precise information which may have been accessed by the threat actor, the information could have included your name, gender, date of birth, telephone number(s), address, social security number, all employment (W-2) information, 1099 information, as well as direct deposit bank account information, including account number and routing information (if provided to us). Further, the information may have included supporting documentation such as brokerage statements and other types of specific documents you may also have provided to us.

For Entities: While our investigation has not revealed the precise information, which may have been accessed by the threat actor, the information could have included your company name, Federal Employer Identification Number, address, telephone number; employee and/or 1099-recipient information, partner, shareholder/officer or beneficiary names, addresses, social security numbers; and/or other information you may have also provided to us.

What We Are Doing
With the assistance of our IT consultants, the following steps have been taken: (1) immediate enhancements to our systems, security, and practices have been implemented to prevent unauthorized access in the future; (2) all network passwords have been changed; and (3) two-step authentication has been implemented for online system access. We will continue to work with our IT consultants to keep the firm and clients safe from a future security breach.

Further, we are working with the appropriate agencies on your behalf such as the IRS. The IRS is monitoring our firm's client tax filings to ensure heightened security of those returns.

In response to the incident, we are providing you with access to **Triple Bureau Credit Monitoring** services at no charge. These services provide you with alerts for 12 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. 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.

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: [redacted]

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.

What You Can Do

If you choose not to use these services, we strongly urge all customers to consider doing the following:

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)	**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

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.
- You may also want to consider contacting these three credit agencies at the phone numbers above to place a credit freeze on your credit file for free. A credit freeze means potential creditors cannot get your credit report, making it less likely that an identify thief can open new accounts in your name. Find your State Attorney General's Office at https://www.naag.org/find-my-ag/ to learn more.
- Be sure to promptly report any suspicious activity to Daniel E. Fitzgerald, CPA.

- We strongly recommend you be vigilant in reviewing your bank account and brokerage statements, as well as free credit reports to spots signs of fraud or identify theft.
- We suggest you change any bank account numbers provided to us, and/or have a conversation with your bank regarding the monitoring they can provide. It is also recommended that you change your passwords on all accounts, bank and brokerage.
- We also suggest you contact the Federal Trade Commission at 1-877-438-4338 and the Social Security Administration at 1-800-772-1213 about getting an Identity Protection PIN to use with your Social Security Number that criminals do not know. The FTC also provides information online at: www.ftc.gov/idtheft. If you suspect identity theft, report it to law enforcement, including the Federal Trade Commission at https://www.identitytheft.gov/#/assistant and your State Attorney General's Office at https://www.naag.org/find-my-ag/.
- Lastly, you can also obtain information from the Federal Trade Commission about fraud alerts and security freezes. 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/

The protection and privacy of your information has always been a top priority for our firm. After our many years—and sometimes decades—of close business relationships with our clients, we have no words to express how devastating it is to have had this happen. We extend our deepest apologies for any inconvenience this incident may have caused you.

For More Information

Representatives are available for 90 days from the date of this letter, 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. Please call 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

At Daniel E. Fitzgerald, CPA, we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Daniel E. Fitzgerald, CPA

Daniel E. Fitzgerald, CPA