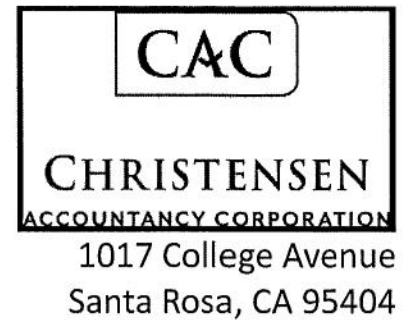


A

<Return Name>
<Return Address>
<City> <State> <Zip>



<<Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>

October 7, 2022

Dear: <<Name>>

Please read this letter in its entirety.

We are writing to inform you of a security incident that may have resulted in the disclosure of your personal information. We recently became aware of a situation where an unauthorized party accessed one of our employee's email accounts. We discovered this situation on **March 26, 2022** and took immediate steps to shut down access to the account. We promptly engaged our IT support to help us investigate, evaluate, and respond to the situation.

While we have no evidence that any of your personal information was misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What information was involved?

Based on our IT's review of the situation and an examination of the impacted email account, it is possible that some personal data belonging to you was potentially exposed to the unauthorized intruder. This data may have included personally identifiable information (PII) with some combination of your name, address, and social security number

What is Christensen Accountancy Corporation doing to address this situation?

Christensen Accountancy Corporation has made immediate enhancements to our systems, security, and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward. We are committed to helping those people who may have been impacted by this unfortunate situation.

In response to the incident, we are providing you with access to the following services:

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 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/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. Cyber monitoring will look out for your personal data on 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 event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

* 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.

How do I enroll for the free services?

To enroll in Credit Monitoring* services at no charge, please log on to <https://secure.identityforce.com/benefit/CAC> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<CODE>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What can I do on my own to address this situation?

Representatives have been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts. If you choose not to use these services, we strongly urge you to do 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)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
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.
- Be sure to promptly report any suspicious activity to Christensen Accountancy Corporation

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

What if I want to speak with Christensen Accountancy Corporation regarding this incident?

While the call center representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Christensen Accountancy Corporation regarding this incident. If so, please call Linda Lemus at (707) 546-8512 from (10:00 a.m. – 3:00 p.m.) Pacific time, Monday through Friday.

At Christensen Accountancy Corporation we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Dan J. Christensen, Jr.

Dan J. Christensen, Jr.
C.P.A.

* 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.