A

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

CAC
CHRISTENSEN
ACCOUNTANCY CORPORATION
1017 College Avenue
Santa Rosa, CA 95404

<<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)	**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.
- 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.

m

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

CAC
CHRISTENSEN
ACCOUNTANCY CORPORATION
1017 College Avenue
Santa Rosa, CA 95404

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

October 7, 2022

Dear Parent or Guardian of: <<FirstName>> <<LastName>>

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 child's 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 child's 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:
In addition, I am providing the parents of impacted minor dependents with access to **Cyber Monitoring*** services at no charge for twelve months from the date of enrollment. Cyber monitoring will look out for your child's personal data on the dark web and alert you if your child's personally identifiable information is found online. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring services at no charge, please log onto **https://secure.identityforce.com/benefit/CAC** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<Code>>** Once you have enrolled, you will click on "Child Monitoring" and enter the information for the child that you are wanting to be included in the monitoring. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

* 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.

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

If you choose not to use these services, we are strongly urging all parents to contact the credit bureaus and ensure no credit file exists in the name of your minor child. Representatives have been retained to help you with any questions or problems you may encounter.

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.
- 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.

D

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

CAC
CHRISTENSEN
ACCOUNTANCY CORPORATION
1017 College Avenue
Santa Rosa, CA 95404

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

October 7, 2022

To the Estate of: <<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 our clients' 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.

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 our clients was potentially exposed to the unauthorized intruder. This data may have included personally identifiable information (PII) with some combination of client names, addresses, and social security numbers.

Please note, however, that since becoming aware of this incident, we have received no indication that your kin's information has been used by the unauthorized actor or by any unauthorized party to commit fraud. We are providing notice of this incident to you out of an abundance of caution.

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.

What can you do to address this situation?
Enclosed with this letter you will find additional information regarding the resources available to you, and the steps that you can take to further protect your kin's personal information. We encourage you to remain vigilant against incidents of identity theft and fraud. Such vigilance includes reviewing account statements and credit reports for suspicious activity to the affiliated institutions immediately.

Other Important Information
You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). 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.

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Furthermore, to help protect your deceased family member, there are steps you can take to request a copy of your deceased family member's credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report. An executor or surviving spouse can also request that the following two notices be placed on a deceased individual's credit report:

- "Deceased – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – notifying the relationship)."

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

For more information regarding identity theft and the deceased, please visit http://www.idtheftcenter.org and search for "FS 117 - Identity Theft and the Deceased - Prevention and Victim Tips." You should also notify the Social Security Administration and Internal Revenue Service of the death of your family member and that you received this letter.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or

- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.
The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.