WILLIAMS ADAMS
& COMPANY, CPAs

Dear Client,

We are writing to provide you with a formal notification regarding a data incident involving Williams Adams & Company, CPAs' network computers, 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 July 28, 2022, we discovered that our network servers were encrypted by an unauthorized user, preventing our firm's ability to access the network and resulting in a complete operational outage of our system. Shortly thereafter the threat actor contacted our office, stating that they would only decrypt the network in exchange for a large sum of money. We immediately engaged a forensic IT consultant to decrypt the network and/or restore it using our backup drives, and to also determine what, if any, information on our network was accessed by the threat actor.

On August 5, 2022, our forensic IT consultant determined that he could not decrypt the network or otherwise recover the information therein. As such, we were forced to negotiate with and pay the threat actor to recover the data on our network. Following payment of a ransom sum, our network was decrypted on August 9, 2022 and we have been working diligently with our IT consultants to restore our systems and gather client contact information to provide the notification herein.

Although our network was encrypted by an unauthorized user, we have no information that your sensitive information was compromised or misused in any manner. We likewise have no information that our EFIN or 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 suspicious activity in connection with your tax returns, we will notify you immediately. Conversely, if you receive any notifications from the IRS concerning your account, please notify our office right away.

What Information Was Involved?

<u>For Individuals:</u> 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 accessed 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 help 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 passwords have been changed; (3) a two-step authentication has been implemented for online system access; and (4) we have engaged experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols, including network firewalls, are in place and properly functioning going forward. 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 and FTB. Our EFIN has been changed and the IRS is monitoring our firm's tax client filings to reject any returns filed fraudulently.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by Cyberscout through Identity Force, a 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 contact Farah Zabrani at (661) 633-9122 or by emailing her at accounting@williamsadams.com. You will be provided a webpage and access 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 You Can Do:

- We strongly recommend you be vigilant in reviewing your bank account and brokerage statements, as well as free credit reports.
- 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. If you suspect identity theft, report it to law enforcement, including the Federal Trade Commission at https://www.identitytheft.gov/Assistant# and the State Attorney General's Office at naag.org.
- We recommend you call one of the three major credit agencies and place a 90-day fraud alert on your accounts. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. To do so, their contact information is:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp	https://www.experian.com/ fraud/center.html	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

- You are also entitled to a free credit report every year from each of these three credit agencies at: www.annualcreditreport.com
- 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. 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. The cost to place and lift a freeze depends on state law. Find your State Attorney General's Office at naag.org to learn more.
- 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:

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. If you have any questions or concerns, call Farah Zabrani, at 661-633-9122, or email at accounting@williamsadams.com; or write 5558 California Avenue, Suite 208 Bakersfield, CA 93309.

Sincerely,

Williams Adams & Company, CPAs