Carmel Minogue CPA & Associates, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
AARON B DUNNINGTON
642 CEDARWOOD DR
POWELL, WY 82435

LEWISTON
77 SOUTHWAY AVE, STE B,
LEWISTON, ID 83501
P: 208-743-7790 F: 208-743-7363

MOSCOW
610 S MAIN ST, MOSCOW ID 83843
P: 208-882-0288

PULLMAN
105 E MAIN ST, PULLMAN, WA
99163
P: 509-332-1225 F: 509-332-2413

May 14, 2024

NOTICE OF DATA BREACH

P 0000101102G0400

Dear Aaron B Dunnington,

I am writing to provide you with a formal notification regarding a data incident occurring at Carmel Minogue CPA & Associates, during which your personal 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 February 23, 2024, we learned that an unauthorized user hacked ConnectWise, a remote access program used by our firm to provide remote technical support on client systems. The attack on ConnectWise allowed the threat actor to gain access to and install ransomware on our firm's network computers.

Upon learning this information we immediately notified our IT department, which shut down our office's server and contacted ConnectWise to ensure any unauthorized access through the ConnectWise software was terminated. With the help of our IT department and our forensic technology consultants, we engaged in a thorough investigation concerning the scope of the ConnectWise breach and the source of the ransomware. Unfortunately, through our investigation, we learned that your sensitive personal information may have been accessible to the perpetrator of this crime. We also learned that this incident was part of a large-scale cyber attack of various customer systems through the exploitation of the ConnectWise program.

Although we have no information that your sensitive data has been misused in any manner, we are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have. If you receive any notifications from the IRS concerning suspicious activity on your tax account, please notify our office right away.

What Information Was Involved?

For Individuals: The information accessed by the threat actor may have included your name, gender, date of birth, telephone number(s), address, social security number, all employment (W-2) information, and 1099 information. Further, the information may have included supporting documentation such as brokerage statements and other types of documents you may also have provided to us.

For Entities: The information accessed by the threat actor may 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; (3) two-step authentication has been implemented for online system access; (4) use of the ConnectWise software has been terminated pending information from ConnectWise, Inc. that all security vulnerabilities have been corrected. 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, including the IRS. The IRS is monitoring our firm's client tax filings to ensure heightened security of those returns. This notification to you was not delayed as a result of a law enforcement investigation.

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 through Identity Force, 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: 64D09C239A69

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:

- We strongly recommend you be vigilant in reviewing your bank accounts and brokerage statements, as well as free credit reports.
- We recommend you use one of the three major credit agencies below to 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.

Equifax	**Experian**	**TransUnion**
P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	P.O. Box 2002 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

- You may also want to consider contacting these three credit agencies at the telephone 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. Pursuant to the federal Fair Credit Reporting Act, there is no cost to place or lift a credit freeze. Find your State Attorney General's Office at https://www.naag.org/find-my-ag/ to learn more.
- You are also entitled, pursuant to the federal Fair Credit Reporting Act, to a free credit report from each nationwide credit bureau and from nationwide specialty consumer reporting agencies once every 12 months; and you are entitled to dispute incomplete or inaccurate information. You may obtain your free credit report from each of the three major credit reporting agencies at www.annualcreditreport.com.
- We also suggest you contact the IRS about getting an Identity Protection PIN to use with your Social Security Number for heightened security. You can do this by going to https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.
- If you suspect identity theft, report it to law enforcement, including the Federal Trade Commission at https://www.identitytheft.gov/#/ and your State Attorney General's Office, which can be found 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 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/

00001020280000 P

The protection and privacy of our clients' and their employees' information has always been a top priority for our company. 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 Cyberscout, at 1-833-547-6243 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Sincerely,

Carmel Minogue, CPA
Carmel Minogue CPA & Associates, Inc.