DATAMATE™
BOOKKEEPING & TAX, INC

Notice of Data Breach

Gilroy, California – February 15, 2024 - Datamate Bookkeeping & Tax, Inc. ("Datamate") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to some individuals' sensitive personal information. This notice is intended to provide details about the incident, steps we are taking in response, and resources available to help protect against the potential misuse of sensitive personal information.

What Happened?

On December 10, 2023, Datamate became aware of suspicious activities on its network. Datamate immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on January 25, 2024 and determined that some of Datamate files were accessed by an unauthorized actor.

Based on these findings, Datamate began reviewing the affected files to identify the specific individuals and the types of information that may have been compromised. While this process remains ongoing, Datamate will notify affected individuals by mail as the information becomes available.

What Information Was Involved?

Based on the investigation, the following information related to potentially impacted individuals may have been subject to unauthorized access: name, Social Security Number, tax identification number, driver's license number or state issued identification number, student identification number, financial account number, bank account number, health insurance policy number, date of birth, and / or emails in combination with a password that would permit access. For a small number of full-service clients, passwords required to access bank accounts were also potentially compromised.

Please note that the information above varies for each potentially impacted individual. Affected individuals will be notified by mail of information that was impacted.

What We Are Doing:

Data privacy and security is among Datamate's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, Datamate moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, Datamate engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident.

Additionally, Datamate took the following steps, including, but not limited to: migrated all customer data off the legacy IT systems and into a secure, cloud-based platform protected with multifactor authentication and encryption; moved to new work personal computers, all of which are protected by

encryption and multifactor authentication; all company IT systems are running endpoint security tools, monitored by a third party; upgraded the company network with enhanced network monitoring and security; enhanced security measures for company email accounts; transitioned the tax filing systems to cloud-based systems; implemented access restrictions to Datamate's information systems; and provided all employees with cyber-security and compliance training.

In light of the Incident, we are also providing affected individuals with complimentary monitoring and identity theft restoration services. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

Datamate encourages clients to change their passwords for all their financial and bank accounts if those passwords have been shared with Datamate.

Datamate also encourages all individuals to contact the IRS to request an annual filing PIN and to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

Other Important Information:

We recognize that you may have questions not addressed in this notice. Please call the toll-free help line 1-833-770-0825 and Representatives are available for 90 days from the date of this letter, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding U.S. holidays to assist you with questions regarding this incident and to provide you with a code for complimentary monitoring and identity theft protection services.

Datamate apologies and sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Janel L. Quintos, CEO
Datamate Bookkeeping & Tax, Inc.

DATAMATE™
BOOKKEEPING & TAX, INC

7881 Church Street, Suite F • Gilroy, CA 95020
P: 408-848-2293 • F: 408-848-3034 • datamatebookkeeping.com

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.

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

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You 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:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com/fraud/center.html	www.transunion.com/fraud-alerts	https://www.equifax.com/personal/credit-

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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *New Mexico*: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the ~~Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf~~ or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of *Oregon*: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

~~**For residents of *Vermont:*** If you do not have internet access but would like to learn more about how to place a~~ security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-~~2424 toll free in Vermont only).~~

For residents of *Rhode Island*: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of *Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina,* and *Rhode Island:* You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov
Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov
Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-9995630; www.illinoisattorneygeneral.gov
Maryland Office of the Attorney General - you may also may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

New York Office of Attorney General - you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina Office of the Attorney General - the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1401-274-4400; www.riag.ri.gov