



June 12, 2024

Jennifer S. Stegmaier  
312.821.6167 (direct)  
Jennifer.Stegmaier@wilsonelser.com

Via Certified Mail Receipt Requested

RECEIVED

JUN 18 2024

CONSUMER PROTECTION  
DIVISION

Attorney General Raúl Labrador  
Office of the Attorney General  
Attn: Security Breach Notification  
700 West Jefferson Street, Suite 210  
P.O. Box 83720  
Boise, Idaho 83720-0010

**Re: Notice of Data Breach Involving Datamate Bookkeeping & Tax, Inc.**

Dear Attorney General Labrador:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Datamate Bookkeeping & Tax, Inc. (“Datamate”), a company that provides bookkeeping, accounting, and tax services for businesses and non-profit organizations, located at 7881 Church Street, Suite F, Gilroy, California 95020, with respect to a recent cybersecurity incident that was first discovered by Datamate on December 10, 2023 (hereinafter, the “Incident”). Datamate takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Idaho residents being notified, and the steps that Datamate has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

**1. Nature of the Incident**

On December 10, 2023, Datamate became aware of suspicious activities on its network. An unauthorized third party attempted to infiltrate Datamate’s network and gained access from September 23, 2023 to December 10, 2023. Upon learning of this incident, 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’s 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. During the review process, Datamate proceeded with Substitute Notice by posting notice of this Incident on its website on February 15, 2024 and published media notice in the San Francisco Chronicle on February 25, 2024. On June 3, 2024, Datamate finalized the list of individuals to notify.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston  
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans  
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

Based on its investigation, the personal information that may have been compromised included: first and last name; address; date of birth; Social Security number; tax identification number; passport number; permanent residency card; driver's license number or state-issued identification; student identification number; financial account information (bank account number and routing number). For a small number of full-service clients, passwords required to access bank accounts were also potentially compromised. The information varied by individual.

## **2. Number of Idaho residents affected.**

A total of 3 Idaho residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on June 12, 2024, by first class mail. A sample copy of the notification letter is included with this letter as **Exhibit A**.

## **3. Steps taken in response to the Incident.**

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.

Datamate offered 12 months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, to all affected individuals to help protect their identity. Additionally, Datamate provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

**4. Contact information**

Datamate remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Jennifer.Stegmaier@wilsonelser.com or 312.821.6167.

Very truly yours,  
**Wilson Elser Moskowitz Edelman & Dicker LLP**



Jennifer S. Stegmaier

**EXHIBIT A**  
**(Sample Copy of Individual Notice Letter)**

Datamate  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998  
**Via First-Class Mail**  
P



SANTA NELLA, CA 95322

June 12, 2024

**Re: Notice of Data Breach**

Dear \_\_\_\_\_,

Datamate Bookkeeping & Tax, Inc. (“Datamate”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. This notice is intended to provide you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

**What Happened?**

On December 10, 2023, Datamate became aware of suspicious activities on its network. An unauthorized third party attempted to infiltrate Datamate’s network and gained access from September 23, 2023 to December 10, 2023. Upon learning of this incident, 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’s 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. During the review process, Datamate proceeded with Substitute Notice by posting notice of this Incident on its website on February 15, 2024 and by publishing notice in a statewide media outlet on February 25, 2024. On June 3, 2024, Datamate finalized the list of individuals to notify.

**What Information Was Involved?**

Based on the investigation, the following information related to you may have been subject to unauthorized access: first name, last name, address, social security number, date of birth, bank account number, routing number.

**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 you with 12 months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

### **What You Can Do**

Datamate encourages clients to change their passwords and/or account numbers for their financial and bank accounts if those account numbers and 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.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is 09/30/2024.

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:

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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

### **For More Information**

If you have any questions or concerns not addressed in this letter, please call 1-833-770-0825 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Datamate 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 Quintos, CEO  
Datamate Bookkeeping & Tax, Inc.

## 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](http://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

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

### TransUnion

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

### Equifax

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**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

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

### TransUnion

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

### Equifax

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**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](http://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](http://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 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](http://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](http://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](http://www.oag.dc.gov)

**Illinois office of the Attorney General -** 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General - Consumer Protection Division:** 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General - Consumer Frauds & Protection:** The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General - Consumer Protection Division:** 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General - Consumer Protection:** 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)