Turbo Data Systems
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Jane A Smith Jr
123 Main St
Apt A
Sample, XX ABC12 DE34

September x, 2026

Subject: Notice of Data Breach

Dear Jane A:

We are writing to inform you of a data event that may have affected your personal information. Turbo Data Systems (TDS) provides processing services for agencies and municipalities throughout California, including [agency]. TDS values privacy and security of all information within its possession. This letter contains information regarding the incident, our response, and steps that you can take to protect your personal information.

What Happened? On November 21, 2025, we determined some of your information may have been involved in the event. In November 2024, TDS experienced a network disruption that interrupted services. We immediately investigated with support from cybersecurity specialists. From the investigation, we determined some files related to citation payment services may have been accessed without authorization around November 21, 2024. We conducted a comprehensive and exhaustive review to determine the specific information present so we could notify applicable individuals. As part of the investigation, on November 21, 2025, we learned some of your information may have been involved in the incident, which is the reason for this notification. After completing the review, we worked with [agency] to confirm contact information so we could notify you.

What Information Was Involved? The information may have included your name and Social Security number. Please note we have no evidence any of this information was used to commit identity theft or fraud.

What We Are Doing. As soon as TDS discovered this incident, we investigated immediately and took the steps described above to confirm our network security and to determine the scope of the event. We notified the FBI and will cooperate with any resulting investigation. Additionally, we are providing you with the opportunity to enroll in complimentary credit monitoring and identity protection services, including a $1,000,000 identity theft insurance policy at no charge to you. These services provide you with alerts for 12 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in the credit monitoring and identity protection 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: **ABC123DEF456**. 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. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you throughCyberscout, a TransUnion company] by using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1 877-344-7618 Monday through Friday from 8:00 am to 8:00 pm ET, excluding holidays.

Sincerely,

Turbo Data Systems
1551 N. Tustin Ave, 950
Santa Ana, CA 92705

Draft

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. You have the right to request any police report filed in response to this incident.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

F**or Additional Information:** You have the right to obtain any police report filed related to this matter. You can obtain additional information by contacting the Federal Trade Commission at 600 Pennsylvania Ave, NW, Washington, DC 20580; consumer.ftc.gov; 877-438-4338. Residents of the below states can obtain additional information about the steps you can take to avoid identity theft:

- District of Columbia Attorney General, 400 6th Street, NW, Washington, DC 20001; oag@dc.gov; 202-727-3400.
- Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; https://www.marylandattorneygeneral.gov/or 1-410-528-8662 or 1-888-743-0023.
- New York Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov; or 1-800-771-7755. New York Bureau of Internet and Technology, 28 Liberty Street, New York, NY 10005; www.dos.ny.gov/consumerprotection; 212-416-8433.
- North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; https://ncdoj.gov; and toll-free at (877) 566-7226 or (919) 716-6000.
- Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; www.riag. ri.gov or 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in this matter. There are approximately [XX] Rhode Island residents potentially impacted by this incident.

Draft