

ACME Truck Line, Inc.
c/o Cyberscout
<<Return Address Mail>>



«FirstName» «LastName»
«Address1» «Address2»
«City», «State» «PostalCode+4»

April 30, 2026

RE: Important Security Notification. Please read this entire letter.

Dear «FirstName» «LastName»:

ACME Truck Line, Inc. (“ACME”) recently discovered an incident that may affect the security of your personal information. We want to provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so. You are receiving this letter because ACME’s records show you worked with ACME.

What Happened? On February 19, 2026, ACME discovered that an unauthorized third party gained access to certain computer systems maintained by ACME (the “Cyber Attack”). The Cyber Attack was carried out by an unauthorized person who exploited vulnerabilities in third-party security services and software used to protect ACME’s network. A third-party vendor retained to monitor ACME’s network for threats of this kind did not identify or escalate indicators of the attack before it was executed. Upon discovering the Cyber Attack, ACME acted immediately to contain the incident, engaged a forensic cybersecurity firm to investigate, and notified law enforcement.

What Information Was Involved? The personal information that may have been accessed or acquired as a result of the Cyber Attack includes your name in combination with one or more of the following data elements: Social Security number; date of birth; driver’s license number; financial account and/or direct deposit information; tax withholding records; and health insurance enrollment information.

What We Are Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Upon discovering the Cyber Attack, ACME engaged a forensic cybersecurity firm to investigate the scope and nature of the incident and notified the Federal Bureau of Investigation. ACME has also undertaken a comprehensive review of its security environment, including the performance of its third-party security vendors, and has implemented additional safeguards to strengthen its defenses against future attacks, including strengthened vendor oversight protocols, enhanced Endpoint Detection and Response tools, improved network firewalls, mandatory Multi-Factor Authentication, expanded user password policies, and third-party testing to scan systems for vulnerabilities and validate cyber-security best practices.

In response to the incident, we are providing you with access to Three Bureau Credit Monitoring, Credit Report, and Credit Score services at no charge. These services provide you with alerts for 24 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. Finally, 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.

How do I enroll for the free services? To enroll in these services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the unique activation code listed below 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. 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.

If you believe you have been a victim of identity theft or fraud related to this incident, a personal fraud specialist is available to assist you. See the “Identity Theft and Fraud Resolution Services” details below.

To activate your credit monitoring and identity protection services, please follow the steps below:

- Enroll within 90 days from the date of this letter (your code will not work after that date).
- **Visit the TransUnion enrollment site at <https://bfs.cyberscout.com/activate>.**
- Provide your **activation code**: «UniqueCode»

If you have questions about the product, need assistance with fraud resolution arising from this incident, or would like an alternative to enrolling online, please call the help line at 1-833-289-3091, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern time (excluding holidays), and supply the fraud specialist with your unique activation code listed above. You must call within 90 days from the date of this letter. A credit card is not required for enrollment. Once enrolled, you will have access to the following features for 24 months:

- **Credit Monitoring:** TransUnion will monitor activity associated with your identity as it relates to changes on your credit report and alert you to these changes.
- **Credit Report:** You will receive a TransUnion credit report each month through your online dashboard. This service does not prevent you from receiving a free credit report every 12 months directly from a credit reporting agency.
- **Credit Score:** You will receive a monthly TransUnion credit score, including your current score, lender’s view rating, and high-level score factors.
- **Identity Theft and Fraud Resolution Services:** If you fall victim to identity theft as a result of this incident, you will have unlimited access to a personal fraud specialist who can assist with creation of a Fraud Victim affidavit, preparation of documents needed for credit grantor notification, notification to relevant government and private agencies, filing a law enforcement report, comprehensive case file creation for insurance and law enforcement, placement of credit file freezes (where available), and review of credit reports for possible fraudulent activity.
- **Proactive Fraud Assistance:** A fraud specialist will work with you one-on-one to answer questions and concerns related to identity protection best practices, including assistance with reading and interpreting your credit report, fraud specialist–assisted placement of fraud alerts, and removal from credit bureau marketing lists while a fraud alert is active (United States only).
- **\$1,000,000 Identity Theft Insurance:** Reimbursement for identity theft expenses incurred as a result of an identity theft event that occurs or is first known during the coverage period, including legal expenses, lost wages, loan application fees, notarization and postage costs, and costs to purchase up to six credit reports from any of the three major credit bureaus (Experian, Equifax, or TransUnion). Identity Theft Insurance is not available as a stand-alone product; it is only available in combination with other fraud protection services.

What You Can Do. In addition to enrolling in the credit monitoring and identity protection services described above, we recommend that you take the following steps to protect your personal information:

- **Monitor Your Accounts.** Review your financial account statements and explanation of benefits statements for any unauthorized activity. Report any unauthorized transactions to your financial institution or insurer.
- **Obtain Free Credit Reports.** 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 1-877-322-8228, or writing to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Review your credit reports for any accounts or inquiries you do not recognize.
- **Fraud Alerts and Security Freezes.** You can obtain information from the Federal Trade Commission and the national consumer reporting agencies about fraud alerts and security freezes.
 - **Fraud Alert:** You may place a fraud alert on your credit file by contacting one of the three agencies below. A fraud alert tells creditors to take extra steps to verify your identity before opening a new account.
 - **Security Freeze:** You may place a security freeze on your credit report, free of charge, which prohibits a credit reporting agency from releasing your credit report without your express authorization.
- **Contact information for the three nationwide consumer reporting agencies:**
 - **Equifax:** P.O. Box 105788, Atlanta, GA 30348; 1-800-525-6285; www.equifax.com
 - **Experian:** P.O. Box 9554, Allen, TX 75013; 1-888-397-3742; www.experian.com/freeze
 - **TransUnion:** P.O. Box 2000, Chester, PA 19016; 1-800-680-7289; www.transunion.com/credit-freeze
- **Report Identity Theft.** If you believe you are a victim of identity theft, you may file a report with the Federal Trade Commission at www.identitytheft.gov or by calling 1-877-438-4338. You may also file a report with your state attorney general or local law enforcement. If you are a victim of identity theft, you are entitled to obtain a copy of your credit report free of charge and to have information relating to the fraudulent transactions removed from your credit report.
- **File a Report with Law Enforcement.** You have the right to file a police report if you experience identity theft. Please retain a copy of the police report, as you may need it to clear fraudulent debts. You may also report suspected identity theft to your state attorney general.

For More Information. Please see the Additional Resources for Identity Theft Prevention at the end of this letter for further information on protecting your personal information. Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. and 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-289-3091 and supply the fraud specialist with your unique code listed above.

Sincerely,

/s/ Lance Noël

Lance Noël

IT Program Director

lance.noel@acmetruck.com - 504-361-7060

200 Westbank Expressway, Gretna, LA 70053

Additional Resources for Identity Theft Prevention

You may consider the following additional steps you can take to protect your personal information by contacting the following agencies and resources:

- **Federal Trade Commission:** Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-ID-THEFT (438-4338); www.identitytheft.gov.
- **For California residents:** You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.
- **For Colorado residents:** Office of the Colorado Attorney General, 1300 Broadway, 10th Floor, Denver, CO 80203; 1-800-222-4444; www.coag.gov.
- **For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- **For District of Columbia residents:** the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.
- **For Illinois residents:** You may contact the Illinois Attorney General's Office, Consumer Fraud Bureau, 500 South Second Street, Springfield, IL 62701; 1-800-386-5438; <https://illinoisattorneygeneral.gov>.
- **For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- **For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023.
- **For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.
- **For New Mexico residents,** consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting 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 New York residents:** New York Office of the Attorney General: The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov>. New York Department of State (Division of Consumer Protection): 99 Washington Avenue, Suite 650, Albany, NY 12231; 1-800-697-1220; <https://dos.ny.gov/consumer-protection>.
- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.
- **For Virginia residents:** You may contact the Office of the Virginia Attorney General, 202 North 9th Street, Richmond, VA 23219; 1-804-786-2071; www.oag.state.va.us.