Ampex Data Systems Corporation
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

May x, 2026

RE: Important Security Notification. Please read this letter in its entirety.

Dear <<First Name>> <<Last Name>>:

We are writing to provide you with information about a cybersecurity incident involving Ampex Data Systems Corporation. You are receiving this email because, as a past or present contractor, employee or dependent of Delta Information Systems, Inc., or one of our subsidiaries, including Ampex Data Systems Corporation, Acroamatics, Inc., Telemetry and Communications Systems, Inc., or Wideband Systems, Inc. your information may have been impacted.

What Happened?

On March 21, 2026, we learned that a threat actor group had accessed and encrypted the network at one of our office locations. We immediately informed our IT Security Consultants and shut down our servers. We also engaged with a specialized Forensic IT firm and Cyber Counsel to investigate and remediate the situation. These experts worked with our IT personnel to assess the scope of the situation and to recommend additional security measures. The forensic team confirmed the unauthorized access to our servers on March 21, 2026. The forensic experts contained the incident on March 23, 2026, but the restoration process of our network and servers is still on-going. While the forensic experts confirmed that the threat actor group gained access to the data on our network, the full extent was not known until May 9, 2026.

Based upon the forensic investigation and analysis, we believe that the personal information of a number of our current and former corporate contractors, employees, and dependents was involved. This information may have included personally identifiable information (PII) with some combination of your name, address, social security number, and/or date of birth. In a limited number of instances, driver's license or banking information may have also been involved.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What Are We Doing?

In addition to the steps outlined above, we notified the FBI's Internet Crime Complaint Center (IC3) and the Department of Defense Cyber Crime Center (DC3). We worked with an incident response service to negotiate with the threat actors to prevent the release of any information. To the best of our knowledge, any release was prevented or minimized. We have engaged an IT Security firm to assist us in restoring our servers and improving our IT Security posture going forward. We are also reviewing our IT policies and procedures to ensure all security measures are in place to improve the security of our information network and related systems and to prevent such an incident from occurring again. Lastly, we are continuing to work with the FBI to assist in its investigation and have updated our IC3 and DC3 reports.

What can Ampex do to help?

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for <<Service Length>> 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 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: **<UniqueCode>**. 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 can I do on my own to address this situation?

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a free fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Ampex

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For more information about what you can do to protect yourself, please review the attached **Information About Identity Theft Protection.**

What if I want to speak with the company regarding this incident?

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. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-877-424-7916 and supply the fraud specialist with your unique code listed above.

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with someone at Ampex regarding this incident. If so, please call Human Resources at 1-650-367-3259 from 9:00AM – 5:00PM Eastern Time, Monday through Friday.

At Ampex, we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Ampex Data Systems Corporation

Information about Identity Theft Protection

For residents of all states:

Fraud Alerts: It is both recommended and required by certain state laws (Michigan, Missouri, Virginia, Vermont and North Carolina) to advise you of your right to place Fraud Alerts with one of the three major credit bureaus by phone and via TransUnion's, Experian's or Equifax's website. 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. Initial Fraud Alerts last for one year. Victims of identity theft can also get an extended Fraud Alert for seven (7) years. Contact information for all three credit bureaus to place a Fraud Alert is listed in your Notice letter.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity. You should also periodically obtain and review a copy of your Credit Report, at no charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one (1) or more of the national consumer reporting agencies listed in the Notice Letter.

You may also obtain a **free copy** of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report **at no cost** to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. Unlike a Fraud Alert, to place a Security Freeze on your credit file, you need to make the request at ***each*** consumer reporting agency individually. You may make that request by 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, 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. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788 Atlanta, GA 30348 https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 https://freeze.transunion.com

For more information on security freezes, you may contact the three nationwide consumer reporting agencies listed in your Notification Letter or the FTC as described below:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (1-877-438-4338), and TTY: 1-866-653-4261, and www.ftc.gov/idtheft.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

ADDITIONAL STATE-SPECIFIC DISCLOSURES & PROTECTIONS.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

> **Office of the Attorney General of Iowa,** Hoover State Office Building,1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5164; www.iowaattorneygeneral.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland residents: You may obtain information about Fraud Alerts, Security Freezes and steps you can take to prevent and avoid identity theft from the Maryland Office of the Attorney General:

> **Maryland Office of the Attorney General,** Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us.

Massachusetts residents: You have the right to obtain a police report with respect 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.

New Mexico Residents. You have rights pursuant to the Fair Credit Reporting Act (FCRA), 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 FCRA: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) 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 by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; 1-800-771-7755.

North Carolina residents: You may obtain information about Fraud Alerts, Security Freezes and steps you can take to prevent and avoid identity theft from the North Carolina Attorney General's Office and the FTC (contact details listed above):

> **North Carolina Attorney General's Office**, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (1-877-566-7226) or 1-919-716-6000 (outside NC); www.ncdoj.gov.

Oregon Residents: You may report suspected identity theft to the Federal Trade Commission (as noted above) or the Oregon Department of Justice / Office of Attorney General and obtain information about Fraud Alerts, Security Freezes and steps you can take to prevent and avoid identity theft at:

> **Oregon Department of Justice, Office of Attorney General,** 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, http://www.doj.state.or.us.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about Fraud Alerts, Security Freezes and steps you can take to protect yourself from identity theft. You can contact the Rhode Island Office of the Attorney General at:

> **Rhode Island Office of the Attorney General,** Consumer Protection Unit, 150 South Main Street, Providence, RI 02903; 1-401-274-4400; http://www.riag.ri.gov.

As noted above, you may obtain a **Security Freeze** on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006. Under Rhode Island law, you also have the right to obtain any police report filed in regard to this event. There was **1** Rhode Island residents impacted by this incident.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001; https://oag.dc.gov/consumer-protection; 1-202-442-9828.