

RECEIVED

MAR 15 2024

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Covington & Burling LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018-1405
T +1 212 841 1000
CONSUMER PROTECTION

By Federal Express

March 14, 2024

Office of the Attorney General
1 Granite Place South
Concord, NH 03301

**Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. Ann.
§ 359-C:20**

To Whom It May Concern:

In accordance with the above-referenced provision of New Hampshire law, I write in connection with an information security incident involving Ultra Electronics Advanced Tactical Systems, Inc. ("ATS").

On November 24, 2023, ATS became aware of a cyber incident involving the use of compromised credentials, through which an unauthorized actor gained access to certain ATS systems. Upon detecting the incident, ATS took immediate steps to isolate the affected systems and disrupted the actor's acquisition of data. ATS immediately launched a comprehensive investigation with the assistance of technical experts and began a process to identify affected individuals. ATS has also been cooperating with law enforcement about this incident and took steps to prevent future unauthorized access, including implementing a global password reset and enhancing monitoring of its network.

As part of the investigation, ATS conducted a comprehensive review of the affected information, including to retain a vendor to review the impacted files and to identify affected individuals. ATS began reviewing affected information on December 19, 2023, while still working to identify the full scope of affected information. On December 27, 2023 the affected information was posted on a website that is not readily accessible to the general public, and ATS finished identifying the full scope of affected information on January 11, 2024. The review was completed on February 20, 2024, and ATS determined on February 21, 2024 that the information included a of a New Hampshire resident.

ATS has identified and plans to notify one (1) resident of New Hampshire. Enclosed is a copy of the notification letter that will be sent to this individual via first-class mail on March 15, 2024.

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by ATS to protect personal information from further unauthorized access; (3) an address and toll-free phone number to call for further information and assistance; (4) information on how the individual may enroll in free credit

COVINGTON

Micaela McMurrough

March 14, 2024

Page 2

monitoring and other complimentary services; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission, and a statement that individuals can obtain information on identity theft from this source; and (8) advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please contact me by phone at

Respectfully submitted,

Micaela McMurrough

Enclosure

ULTRA Intelligence & Communications

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589



L0241-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



March 15, 2024

NOTICE OF DATA BREACH

We are contacting you regarding an incident through which some of your personal information was impacted. On February 21, 2024, we determined that an unauthorized third party acquired some of your personal information. This determination followed an investigation into unauthorized access to Ultra Electronics Advanced Tactical Systems, Inc.'s ("ATS", d/b/a "Ultra Intelligence & Communications") network, which likely occurred between November 1 and November 24, 2023.

What Happened?

On November 24, 2023, we detected suspicious activity on ATS' network and immediately took steps to contain the activity and investigate the incident. The investigation determined that an unauthorized actor gained access to certain systems on our network and acquired certain information, which was later posted on December 27, 2023 on a website that is not readily accessible to the general public. As part of the investigation, we conducted a comprehensive review of the affected information, which was completed on February 20, 2024.

What Information Was Involved?

The information posted included your [Extra1]. We have no indications that the information included your [Extra2].

What We Are Doing.

Upon learning of this incident, we took immediate steps to isolate the affected systems, launch a comprehensive investigation with the assistance of technical experts, and identify affected individuals. We have also been cooperating with law enforcement about this incident and further enhanced our security measures to protect against future incidents.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for _____ from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at _____ by July 1, 2024. Be prepared to provide engagement number _____ as proof of eligibility for the Identity Restoration services by Experian. Additional information describing your services is included in Attachment A.

What You Can Do.

Regardless of whether you elect to enroll in the identity-theft protection service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. Attachment B contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information.

Please be assured that we are taking steps to address the incident and to protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact us at 833-918-8881, Monday – Friday 8 am – 8 pm Central, or at 4101 Smith School Rd. Bldg IV, Ste. 100, Austin, TX 78744.

ATTACHMENT A

ADDITIONAL DETAILS REGARDING YOUR MEMBERSHIP

EXPERIAN IDENTITYWORKS

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information
Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

New York Residents: The Attorney General can be contacted at Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; (800) 771-7755; or <https://ag.ny.gov>.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.