

Notice of Data Breach

United Service Companies (“United”) is providing notice of a recent data security incident affecting personal information. This notice provides information on the incident and what we are doing in response.

What Happened?

We recently discovered that, between on or about October 14 and November 15, 2023, there was unauthorized access to certain United employees’ email accounts. This resulted in a small number of emails being accessed by unauthorized person(s) not affiliated with United and without our knowledge. Therefore, we completed a thorough investigation of the incident, including a detailed review of all potentially affected emails. Through that investigation, we discovered on January 17, 2024, that some of your personal information was contained within the potentially affected emails and, therefore, may have been affected by this incident. We are thus writing to notify you out of an abundance of caution.

What Information Was Involved?

We currently have no knowledge of any actual or attempted misuse of anyone’s personal information. However, through our review of the emails potentially affected by this incident, we have determined that some of them contained personal information, including names and/or Social Security numbers, passport numbers, driver’s license numbers, government issued identification numbers, financial account information, and medical information. Therefore, we notified potentially impacted individuals out of an abundance of caution.

What Are We Doing?

We take the protection of personal information seriously and are taking steps to mitigate the potential for harm and prevent future incidents like this. We changed the login credentials for the affected email accounts and worked with computer forensics experts to ensure there is no continued access to them. In addition, we will continue to work internally and with our IT professionals to review our network and email account policies and procedures to identify other measures that may help strengthen security and prevent future incidents.

What Can You Do?

We recommend that affected individuals remain vigilant by reviewing and monitoring their account statements and credit reports. If you find any errors or unauthorized activity, you should contact your financial institutions that may be affected. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the instructions at the end of this notice titled “Additional Steps to Help Protect Your Information” for more information on protecting your information from misuse.

Additional Safeguards for Affected Individuals

As an additional safeguard, we have arranged for affected individuals to enroll, **at no cost to them**, in 12 months of the online credit monitoring service of *IdentityWorks*, provided by Experian, which is one of the three nationwide credit reporting companies.

Information about how to enroll in this service is provided in written letters being mailed to affected individuals for whom we have available contact information. If you did not receive a letter and believe you may have been affected by this incident, or if you would like to determine if you were affected, please contact our dedicated incident response hotline at (833) 918-1152.

For More Information

We are very sorry for any concern or inconvenience caused by this incident. If you have any other questions or concerns that you would like to discuss, or to determine if you were impacted by this incident, please contact us through our dedicated incident response hotline at (833) 918-1152.

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting

agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or answer security question, you should promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
- **District of Columbia Residents:** District of Columbia Attorney General may be contacted at 400 6th Street, NW, Washinton, D.C. 20001; <https://oag.dc.gov>; and (202) 727-3400.
- **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.marylandattorneygeneral.gov, (888) 743-0023.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know Your Rights Under the Fair Credit Reporting Act. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, which you can read about by visiting <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> and <https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights>. States may enforce the FCRA, and many states have their own consumer reporting laws.