



Freeman
Mathis & Gary LLP

100 Galleria Parkway
Suite 1600
Atlanta, GA 30339-5948

Tel: 770.818.0000

www.fmglaw.com

David A. Cole

D: 770.818.1287
C: 404.805.6558

dcole@fmglaw.com

February 16, 2024

Via Email Only

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: IDtheft@aog.state.md.us

Re: Notice of Data Breach

To Whom It May Concern:

Our firm represents United Service Companies ("United"), a support services provider with its principal office address at 1550 S. Indiana Ave., Chicago, IL 60605. This letter is provided pursuant to the Maryland Personal Information Protection Act, MD. Code Ann. Com. Law §14-3501, *et seq*, which requires notice to the Office of the Attorney General in the event of a breach in the security of personal information affecting residents of the state of Maryland.

United recently learned of suspicious activity involving certain United employees' email accounts. As counsel for United, we directed a thorough, privileged investigation of the activity that included partnering with computer forensic specialists. The investigation found that there was unauthorized access to certain United employees' email accounts that occurred between on or about October 14 and November 15, 2023, which resulted in access to or acquisition of some of the emails and/or files therein. United thus continued the investigation through a comprehensive review of the emails and files to determine if they contained personal information.

Through that process, United discovered on January 17, 2024, that the incident affected the personal information a total of 84 residents of Maryland. The types of personal information affected include Social Security numbers, driver's license numbers, government issued identification numbers, medical information, and financial account information. Although United has no knowledge of any misuse of anyone's information because of this incident, it provided notification to all potentially affected individuals out of an abundance of caution. A sample of the notification letter mailed to residents is enclosed for your records. As reflected therein, United is offering all potentially affected residents free credit monitoring and identity restoration services through Experian IdentityWorksSM.

www.fmglaw.com



Freeman
Mathis & Gary LLP

February 16, 2024

Page 2

United is taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent this from happening again. United 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, United will continue to work internally and with its IT professionals to review its network and email account policies and procedures to identify other measures that may help strengthen security and prevent future incidents.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

A handwritten signature in blue ink, appearing to read "D.A. Cole".

David A. Cole

“Exhibit – A”

(Sample Notification Letter)



February 16, 2024

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

K8716-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Notice of Data Breach

Dear Sample A. Sample:

At United Service Companies (“United”) we take the issue of privacy seriously. As part of that commitment, we are sending you this letter to make you aware of a recent data security incident that may have affected your personal information. Please read this letter carefully.

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 your personal information. However, through our review of the emails potentially affected by this incident, we have determined that one or more of the documents contained your personal information, including your [Extra1]. Therefore, we are notifying you out of an abundance of caution and recommend that you carefully review the information herein.

What We Are Doing

We take the protection of your 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 You Can Do

We recommend that you remain vigilant by reviewing and monitoring your 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 enclosed document “Additional Steps to Help Protect Your Information” for more information on protecting your information from misuse.



As an added precaution to help protect your identity, we are offering complimentary access to Experian's® IdentityWorksSM for a period of 12 months. This product provides you with superior identity detection and resolution of identity theft.

If you believe there was fraudulent use of your information because of this incident and would like to discuss how you may be able to resolve those issues, please contact an Experian agent. If it is determined that identity restoration support is needed, then an Experian agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident, such as helping you contact credit grantors to dispute charges and close accounts, place a freeze on your credit file, or contact government agencies to help restore your identity. These identity restoration services are available to you for 12 months from the date of this letter and do 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 your complementary 12-month membership to Experian IdentityWorks. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by May 31, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration because of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1152 by May 31, 2024. Be prepared to provide engagement number B116585 as proof of eligibility for the Identity Restoration services by Experian.

For More Information

We are very sorry for any concern or inconvenience caused by this incident. If you have any other questions that you would like to discuss, please contact us through our dedicated hotline at 833-918-1152, which is available Monday through Friday from 8 a.m. to 8 p.m. Central. Please be prepared to provide engagement number B116585.

Sincerely,

A handwritten signature in black ink, appearing to read 'Miguel Perez', with a stylized flourish at the end.

Miguel Perez

Vice President, Human Resources

United Service Companies



ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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.¹
- **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 Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 12 months 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.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.



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.



