



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

February 23, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent UNITE HERE located at 275 Seventh Avenue, 16th Floor, New York, NY 10001, and are writing to notify your office of an incident that may affect the security of certain personal information relating to twenty-three thousand one hundred six (23,106) Maryland residents. By providing this notice, UNITE HERE does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 20, 2023, UNITE HERE discovered suspicious activity on certain networks. UNITE HERE promptly took its systems offline and launched an investigation into the nature and scope of the activity. With the assistance of third-party forensic specialists, UNITE HERE investigated this incident to determine whether any sensitive information was viewed or removed from UNITE HERE's systems without authorization. The investigation determined that an unknown actor gained access to certain parts of the network on October 20, 2023.

Following this determination, UNITE HERE worked as quickly as possible to review the documents to determine those individuals whose information was present to notify them about this incident. The review of the impacted data concluded on December 14, 2023. Subsequently, UNITE HERE conducted an additional review to identify the data owners and covered entities associated with the individuals whose data was impacted. After finalizing that list, UNITE HERE notified data owners and covered entities requesting authorization to notify impacted individuals and required regulators on their behalf.

The data owners and covered entities were given two weeks to request additional information and provide authorization.

The information that could have been subject to unauthorized access includes name, Social Security number, medical information, health insurance plan, passport number, driver's license, state identification number, and financial account information. There is no evidence this information has been subject to actual or attempted misuse.

Notice to Maryland Residents

On or about February 23, 2024, UNITE HERE provided written notice of this incident to twenty-three thousand one hundred six (23,106) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, UNITE HERE moved quickly to investigate and respond to the incident, assess the security of UNITE HERE systems, and identify potentially affected individuals. Further, UNITE HERE notified federal law enforcement regarding the event. UNITE HERE is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, UNITE HERE is providing impacted individuals with guidance on how to better protect against identity theft and fraud. UNITE HERE is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

UNITE HERE is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. UNITE HERE is also notifying the U.S. Department of Health and Human Service, and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB/hkl
Enclosure

EXHIBIT A

UNITEHERE!

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<Preferred Name>> <<Name2>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

February 23, 2024

RE: NOTICE OF <<SECURITY INCIDENT / DATA BREACH>>

Dear <<Preferred Name>> <<Name2>>:

On October 20, 2023, UNITE HERE, which handles health and welfare and/or employment data on behalf of certain local unions, health funds, and San Diego UNITE HERE Pension Fund, had an incident that may affect your personal information. We are not aware of any misuse of your information, but out of an abundance of caution, we are writing to let you know what happened, what we have done, and what you can do to protect your personal information if you want.

What Happened? UNITE HERE recently found an unauthorized third-party accessed our systems containing personal information of members and staff from certain local unions, health funds and San Diego UNITE HERE Pension Fund. We immediately took steps to stop the access and increase security. We also brought in cyber specialists to investigate, who found that files may have been taken by the third party on or about October 20, 2023.

What Information Was Involved? The third-party likely accessed information including your name and <<Variable Text 1>>. We currently have no evidence that your information has been misused.

What Are We Doing? The confidentiality, privacy, and security of information in our care is one of our highest priorities. When we discovered this incident, we immediately reset system passwords, added extra layers of security, and investigated what data may be at risk. We also notified law enforcement. We are continuing to work to lower the chances of something like this happening again.

We are also offering <<12/24>> months of complimentary access to credit monitoring services through IDX. Please scan the QR code or call (888) 869-9523 to enroll.

What You Can Do. To be vigilant against identity theft and fraud, we suggest you:

- Review your account statements and credit reports for suspicious activity or errors.
- Review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible information misuse.
- Enroll in the complimentary credit monitoring services we are offering to you by going to <https://app.idx.us/account-creation/protect> or scanning the QR code and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 23, 2024.

D. TAYLOR, PRESIDENT

GENERAL OFFICERS: Gwen Mills, Secretary-Treasurer • Rich Maroko, Recording Secretary
Nia Winston, General Vice President • Enrique L. Fernández, General Vice President for Immigration, Civil Rights and Diversity

For More Information. For questions you may have, or to ask for more information, you can:

- Call our support line (888) 869-9523, Monday through Friday from 9 am - 9 pm Eastern Time.
- Write to UNITE HERE at 275 7th Avenue, 16th Floor, New York, New York 10001.
- Go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

UNITE HERE takes the privacy and security of your information in our care seriously. We sincerely regret any inconvenience or concern this may cause you.

Steps You Can Take to Help Protect Your Information

Enroll in Credit/Identity Monitoring

1. Website and Enrollment. Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (888) 869-9523 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. 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 and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Additional Information

To learn more on these topics and about the credit monitoring agencies, contact the Federal Trade Commission, or your state Attorney General.

- The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.
- The Federal Trade Commission also encourages those who discover misuse of their information to file a complaint with them.
- 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 and your state Attorney General.

This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, 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 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. 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 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, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 67 Rhode Island residents impacted by this incident.

ENGLISH	A translation of this letter is available at the following link: www.unitehere.org/cyber-security/
SPANISH	Una traducción de esta carta está disponible en el siguiente enlace: www.unitehere.org/cyber-security/
FRENCH	Une traduction de cette lettre est disponible au lien suivant : www.unitehere.org/cyber-security/
NEPALI	यस पत्रको अनुवाद तलको लिंकमा उपलब्ध छ www.unitehere.org/cyber-security/
RUSSIAN	Перевод этого письма доступен по следующей ссылке: www.unitehere.org/cyber-security/
AMHARIC	የዚህ ደብዳቤ ትርጉም በሚከተለው አገናኝ ይገኛል: www.unitehere.org/cyber-security/
ARABIC	تتوفر ترجمة هذه الرسالة على الرابط التالي: www.unitehere.org/cyber-security/
HAITIAN CREOLE	Yon tradiksyon lèt sa a disponib nan lyen sa a www.unitehere.org/cyber-security/
OROMO	Xalayaan kun afaan isaatiin barreeffamee kan argamu marsariitii armaan gadii irratti: www.unitehere.org/cyber-security/
SOMALI	Tarjumada warqadan waxaa laga heli karaa xiriirinta soo socota: www.unitehere.org/cyber-security/
TIGRINYA	ናይዚ ደብዳቤ ትርጉም ኣብዚ ዝስዕብ መላግቦ ክትረኽቡዎ ትኽእሉ ኢኹም www.unitehere.org/cyber-security/
UZBEK	Bu xatning tarjimasi quyidagi havolada mavjud: www.unitehere.org/cyber-security/
VIETNAMESE	Bản dịch của bức thư này có sẵn tại liên kết sau: www.unitehere.org/cyber-security/
CHINESE	这封信的翻译可以在以下链接找到 : www.unitehere.org/cyber-security/