

STATE OF NH
DEPT OF JUSTICE

2021 FEB 22 PM 12: 48

BakerHostetler

Baker & Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

William H. Berglund
direct dial: 216.861.7416
wberglund@bakerlaw.com

February 19, 2021

VIA OVERNIGHT LETTER

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, United Food and Commercial Workers Union Local 881 AFL-CIO ("Local 881"), to notify you of a security incident involving two New Hampshire residents. Local 881 is a labor union headquartered in Des Plaines, IL with members based in Indiana and Illinois.

Local 881 has conducted an investigation into an incident involving unauthorized access to some of its Union computer systems on November 6 and 7, 2020. Upon discovering the incident, Local 881 immediately took steps to secure its network, contacted law enforcement, and began an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person accessed certain files on a Union server and potentially transferred at least some of them outside of Local 881's network. Local 881 conducted a thorough analysis of the files that were accessed and potentially acquired to determine if any contained personal information. Although Local 881 initially did not believe that the files would contain information regarding New Hampshire residents, on December 30, 2020, Local 881 determined that the personal information of two New Hampshire residents was contained in the files, including the individuals' names and Social Security numbers.

Beginning today, February 19, 2021, Local 881 will mail notification letters to the New Hampshire residents via First Class U.S. Mail. A sample copy of the notification letter is enclosed.¹ Local 881 is offering the New Hampshire residents a complimentary, one-year membership to

¹ This notice does not waive Local 881's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

February 19, 2021

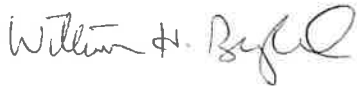
Page 2

credit monitoring and identity theft protection services through CyberScout. Local 881 is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Local 881 has also established a dedicated phone number that the individuals may call with related questions.

To further protect personal information, Local 881 has taken steps to enhance its existing security protocols, including the use of additional antivirus software on all workstations and servers and enhanced technology for remote access to the network. Local 881 is also installing port monitoring software and implementing network monitoring by a professional third-party firm.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

A handwritten signature in cursive script, appearing to read "William H. Berglund".

William H. Berglund
Counsel

Enclosure

ADULT Sample

February 19, 2021

<<First name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip Code>>

Dear <<First name>>:

At Local 881 United Food and Commercial Workers Union, we understand the importance of protecting and securing the personal information that we maintain. I am writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

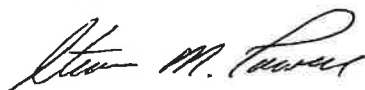
We recently completed an investigation into unauthorized access to some of our Union computer systems at different periods on November 6 and 7, 2020. Upon discovering the incident, we immediately took steps to secure our network, contacted law enforcement, and began an investigation with the assistance of a cybersecurity firm. Our investigation determined that an unauthorized person accessed certain files on a Union server and transferred at least some of them outside of our network. On December 30, 2020, we determined that some of your information was contained in the files that were accessed and/or transferred out of our network by the unauthorized person, including your name and Social Security number.

Although we have no indication to date that your information has been misused, we encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. As an added precaution, we are providing you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Non-Credit Public Records monitoring/Cyber Monitoring*** services at no charge through CyberScout. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition to credit related data, the services will also monitor any changes to your non-credit public records including: Change of Address, Court Records and Social Security number trace. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft.

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Code>>
In order to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we continue to review our systems and are taking steps to enhance our existing security protocols. **If you have any questions, please call 1-800-833-7360 from 9:00 am to 9:00 pm Eastern time, Monday through Friday.**

Sincerely,



Steven M. Powell
President, Local 881 and UFCW International Vice President

* Services marked with an "*" require 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.

INFORMATION ABOUT IDENTITY MONITORING AND FRAUD RESOLUTION SERVICES

We are providing you with access to Triple Bureau Credit Monitoring services at no charge. Services are for 12 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- *Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com
- *TransUnion Security Freeze*, PO Box 2000, Chester, PA 19016, www.transunion.com
- *Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of 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. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.