McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

April 28, 2023

VIA U.S. MAIL

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

Re: USW Local 286 – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents United Steelworkers Local 286 ("USW Local 286") of Philadelphia, Pennsylvania. I am writing to provide notification of an incident at USW Local 286 that may affect the security of personal information of thirteen (13) New Hampshire residents. By providing this notice, USW Local 286 does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

USW Local 286 determined that an unauthorized party obtained access to a USW Local 286 employee email account. Upon learning of the issue, USW Local 286 secured the account and commenced a prompt and thorough investigation. As part of the investigation, USW Local 286 engaged leading cybersecurity experts to identify what personal information, if any, might have been present in the impacted email account.

After an extensive forensic investigation and manual document review, USW Local 286 discovered on February 13, 2023 that the email account, which was accessed between June 16, 2022 and July 18, 2022, contained personal information pertaining to a limited number of New Hampshire residents, such as

. Not all information was included for all individuals.

To date, USW Local 286 has no evidence that any personal information has been misused as a direct result of this incident. Nevertheless, out of an abundance of caution, USW Local 286 wanted to inform your respective Offices (and the affected individuals) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. To that end, USW Local 286 is providing the affected individuals with written notification of this incident commencing on or about April 14, 2023 in substantially the same form as the letter attached hereto. USW Local 286 is offering the affected individuals whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. Further, USW Local 286 is advising the affected individuals about the

process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected individuals are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. The affected individuals whose medical information was impacted are also being provided steps to take to safeguard themselves against medical identity theft.

At USW Local 286, protecting the privacy of personal information is a top priority. USW Local 286 is committed to maintaining the privacy of personal information in its possession and has taken many precaution to safeguard it. USW Local 286 continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at . Thank you for your cooperation.

Sincerely,

James J. Giszczak

Encl.

UNITED STEELWORKERS
USW

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a security incident involving our email system. The privacy and security of the personal information we maintain is of the utmost importance to United Steelworkers Local 286 Union and Benefit Funds ("USW Local 286"). We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

An unauthorized party obtained access to a USW Local 286 employee email account.

What We are Doing.

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. After an extensive forensic investigation and manual document review, we discovered on February 13, 2023 that the email account, which was accessed between June 16, 2022 and July 18, 2022, contained some of your personal information as described in more detail below.

What Information Was Involved?

The accessed email account contained some of your personal information, specifically your [redacted].

What You Can Do.

We have no reason to believe that your information has been misused as a direct result of this incident. Out of an abundance of caution to protect you from potential misuse of your information, we are offering a **complimentary** [redacted] membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary [redacted] membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our toll-free response line at [redacted]. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] Credit Monitoring.

To help protect your identity, we are offering a **complimentary** [redacted] membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [redacted] (Your code will not work after this date.)
2. VISIT the Experian IdentityWor[redacted] to enroll: [redacted]
3. PROVIDE the **Activation Code**: [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [redacted] EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary one - year credit monitoring services, we recommend that you place an initial one (1) year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need toremove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service,you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com.** Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. **Protecting Your Medical Information.**

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392