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

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

May 25, 2018

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

Re: SEIU Local 32BJ – Incident Notification

Dear Mr. MacDonald:

McDonald Hopkins PLC represents SEIU Local 32BJ. I write to provide notification concerning an incident that may affect the security of personal information of 147 New Hampshire residents. 32BJ's investigation is ongoing and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, 32BJ does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

A 32BJ employee was the victim of an email phishing attack via an externally-hosted email management system, resulting in unauthorized access to emails during a 24-hour period from November 13-14, 2017. This incident exposed some personal information of some 32BJ members and other individuals but 32BJ has no evidence that any data has been used inappropriately related to this incident.

Upon learning of the issue, 32BJ initiated a thorough and complex investigation, supported by external cybersecurity experts, to identify the scope of the incident and nature of the impacted data. As a result of this complex and extensive investigation, which concluded on May 18, 2018, 32BJ is now able to confirm that the impacted email account that was accessed contained some personal information of New Hampshire residents, including names and Social Security numbers. 32BJ has no evidence that any of the personal information has been misused.

32BJ wanted to make you (and the affected residents) aware of the incident and explain the steps 32BJ is taking to help safeguard the residents against identity fraud. 32BJ will provide the New Hampshire residents with written notice of this incident commencing on May 25, 2018, in substantially the same form as the letter attached hereto. 32BJ is offering the residents a complimentary membership with a credit monitoring and identity theft protection service and has set-up a dedicated call center to respond to residents' questions. 32BJ will advise the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. 32BJ will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents will also be provided

with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At 32BJ, protecting the privacy and security of personal information is a top priority. To help prevent a similar incident from occurring in the future, 32BJ has enhanced its security policies and protocols, including updating passwords, adding multi-factor authentication, implementing URL protections and revising email attachment scan processes.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

Encl.

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

IMPORTANT INFORMATION

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

At SEIU Local 32BJ, protecting the privacy and security of personal information is a top priority. We value your privacy, which is why I am writing to inform you about a cybersecurity incident involving SEIU Local 32BJ, and to provide you with guidance to protect yourself and share the steps we have undertaken since discovering the incident.

Q. What Happened?

A 32BJ employee was the victim of an email phishing attack via an externally-hosted email management system, resulting in unauthorized access to emails during a 24-hour period from November 13-14, 2017. This incident exposed some personal information of some of our members and other individuals but we have no evidence that any data has been used inappropriately related to this incident.

Q. What is 32BJ Doing in Response?

Since we learned of the issue, we initiated a thorough and complex investigation, supported by external cybersecurity experts, to identify the scope of the incident and nature of the impacted data. As a result of this complex and extensive investigation, which concluded on May 18, 2018, we are now able to confirm that the impacted email account that was accessed contained some of your personal information. While we have no evidence that any of your information has been misused, out of an abundance of caution we are notifying you to provide guidance on what you can do to protect yourself.

To help prevent a similar incident from occurring in the future, we have enhanced our security policies and protocols, including updating passwords, adding multi-factor authentication, implementing URL protections and revising our email attachment scan processes.

Q. What Information of Mine Was Involved?

The impacted email account contained your full name and Social Security number.

Q. What Should I Do Now?

To protect you from potential misuse of your information, we are offering a **free** one-year membership of Experian IdentityWorks℠ Credit 3B, through our existing relationship with one of our service providers and at no additional cost to the Union. 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 should it occur. 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 one-year membership, please see the additional information provided with this letter.

We have also included additional information in this letter regarding other precautionary measures you may want to 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 sincere apologies that this incident occurred and for the stress it might cause.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 9 a.m.- 9 p.m. Eastern Time.

In solidarity,

[redacted]

David Torre
Director of Information Technology Operations
SEIU Local 32BJ

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, we are offering a **complimentary** one-year 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: <<**Enrollment Date**>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [redacted]
3. PROVIDE the **Activation Code**: <<**Enrollment Code**>>

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 [redacted] Be prepared to provide engagement number <<**Engagement #**>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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 [redacted]
or call [redacted] 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 [redacted].

* 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.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "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
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider 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. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

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.

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, Department of Justice, 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.