



Lindsey Smith
100 Light Street, Suite 1300
Baltimore, Maryland 21202
Lindsey.Smith@lewisbrisbois.com
Direct: 410.525.6402

March 16, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

I represent Waterfront Employers-ILA Welfare Fund (the "Fund") administered in Charleston, South Carolina, with respect to a recent data security incident described in greater detail below. The Fund takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the Security Incident.

On January 24, 2022, the Fund mailed W2s to current members and retirees that inadvertently included the information of individuals who were not the intended recipient. Upon discovering this incident, the Fund immediately launched an investigation and engaged a firm to help with notifying impacted individuals. At this time, there is no evidence of misuse of any personal information. Further, we do not have any reason to believe the information has been released outside of other members or retirees. The personal information included names, addresses, and Social Security numbers.

2. Number of Maryland Residents Affected.

The Fund notified one (1) resident of Maryland via first class U.S. mail on March 15, 2022. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident.

The Fund has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps include reviewing the printing configuration that caused the error. Additionally, out of an abundance of caution, the Fund is offering complimentary credit monitoring to all impacted individuals.

4. Contact Information.

The Fund remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 410.525.6402 or via email at Lindsey.Smith@lewisbrisbois.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Lindsey Smith', is centered on the page. The signature is fluid and cursive, with the first name 'Lindsey' written in a larger, more prominent script than the last name 'Smith'.

Lindsey Smith of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Consumer Notification Letter

Waterfront Employers – ILA Welfare Fund

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 15, 2022

Re: Notification of Data Security Incident

Dear <<First Name>> <<Last Name>>,

This letter is to inform you about a data security incident at Waterfront Employers – ILA Welfare Fund (the “Fund”), which may have involved your personal information. As a precaution, we are providing information about steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

What Happened? On the week of January 24th, the Fund mailed W2s to current members and retirees that included the information of individuals who were not the intended recipients. Typically, one individual’s information is printed on one page that includes four copies of that individual’s W2. An error with our automated printing system resulted in four different individuals’ W2 information being included on one page.

As soon as we discovered the incident, we began an investigation and retained a firm to assist us with notifying impacted individuals. At this time, there is no evidence of misuse of any personal information. Further, we do not have any reason to believe the information has been released outside of other members or retirees. We sent you a notification as a precaution so that we could provide you with information about steps you can take to help protect your information.

What Information Was Involved? The information may include: your name, address and Social Security number.

What Are We Doing? All individuals that have been impacted by their information being sent to incorrect addresses, and all individuals who may have received incorrect W2 information are being notified of the error. Additionally, we have taken steps to ensure that the error will not be repeated for future mailings.

Further, we are offering you identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 identity theft insurance policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to enroll in free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> 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 June 10, 2022.

Please call 1-833-903-3648 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

For More Information: Further information about how to protect your information appears on the following page. If you have questions concerning this incident, please contact 1-833-903-3648. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 10, 2022.

Please accept our sincere apologies and know that we deeply regret any concerns or inconvenience that this may cause you. Thank you for your continued trust and support.

Sincerely,

James Bennett

James Bennett
Fund Administrator
Waterfront Employers – ILA Pension and Welfare Fund

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC at **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, D.C. 20580, or online at consumer.ftc.gov and www.ftc.gov/idtheft, or to the Attorney General in your state.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.