



Jason Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
jcherry@constangy.com
207.745.1397

September 10, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy Brooks Smith & Prophete LLP represents Local 1964, International Longshoremen's Association, Local 1964 ILA Health & Insurance Fund, and Local 1964 ILA Retirement Fund ("Local 1964"), located in New Jersey, with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident.

1. Nature of the Security Incident

On May 28, 2024, Local 1964 experienced an encryption event that resulted in a network disruption. Upon learning of the event, Local 1964 took steps to secure its digital environment and engaged third-party experts to investigate. As a result of this investigation, Local 1964 learned that certain data stored in its network may have been acquired between March 27, 2024, and March 27, 2024. Local 1964 then conducted a review of this data, and on September 3, 2024, Local 1964 determined that certain individuals' personal and/or protected health information may have been impacted by this incident.

The affected information included individuals' names, dates of birth, medical information, including provider name and treatment information, health insurance information, and financial account numbers.

2. Number of Maryland Residents Affected

On September 10, 2024, Local 1964 notified five (5) Maryland residents of this incident via first class U.S. mail. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

To help prevent something like this from happening again, Local 1964 is implementing additional security measures and has reported this incident to the Federal Bureau of Investigation. As a further precaution, Local 1964 is offering complimentary identity protection services to all notified individuals.

4. Contact Information

Local 1964 remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at by phone 207.745.1397 or by email at jcherry@constangy.com.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Jason S. Cherry". The signature is fluid and cursive, with a large initial "J" and "S".

Jason Cherry
Partner

Enc.: Sample Consumer Notification Letter



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

<<First Name>> <<Last Name>>
<<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>

September 10, 2024

Subject: Notice of Data <<Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a recent data security incident experienced by Local 1964, International Longshoremen's Association, Local 1964 ILA Health & Insurance Fund, and Local 1964 ILA Retirement Fund ("Local 1964"), located in Ridgefield Park, New Jersey, that may have involved some of your information. This letter is to notify you of the incident, offer you complimentary identity protection services, and inform you about steps you can take to help protect your personal information.

What Happened: On May 28, 2024, Local 1964 experienced an encryption event that resulted in a network disruption. Upon learning of the activity, Local 1964 took steps to secure its digital environment and engaged third-party experts to investigate. As a result of the investigation, Local 1964 learned that certain data stored in its network may have been acquired between March 27, 2024 and May 27, 2024. Local 1964 then conducted a review of this data, and on September 3, 2024, confirmed that your personal information may have been affected by this incident.

What Information Was Involved: The data that could have potentially been accessed by the unauthorized party included your name and <<data elements>>.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures. We are also providing you with information about steps that you can take to help protect your personal information and have reported this incident to the Federal Bureau of Investigation. As a further precaution, we are offering you <<12/24>> months of complimentary identity protection services through IDX. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do: For more information on how you can protect your personal information, please review the resources provided on the following pages. In addition, you can also enroll in the complimentary identity protection services by going to the link noted above or calling the number noted above. When prompted, please provide the unique code noted above to enroll in the services. The deadline to enroll is December 10, 2024.

For More Information: For further information and assistance, please call 1-877-215-7134 between 9:00 am – 9:00 pm Eastern, Monday through Friday.

We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause.

Sincerely,

Local 1964, International Longshoremen's Association
Local 1964 ILA Health & Insurance Fund
Local 1964 ILA Retirement Fund

11 Teaneck Rd.
Ridgefield Park, NJ 07660

Steps You Can Take to Protect Your Personal 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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: 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 or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>

Rhode Island: A total of 4042 individuals are being notified of this incident.