



Sean B. Hoar, Partner & Chair
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, OR 97035
shoar@constangy.com
Mobile: 503.459.7707

June 7, 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:

We represent the Union of California State Workers dba Local SEIU 1000 ("Local SEIU 1000") headquartered in Sacramento, California, with respect to a recent data security incident described below. The purpose of this letter is to provide formal notice to your office.

1. Nature of the Security Incident

On January 18, 2024, Local SEIU 1000 experienced a network disruption and immediately initiated an investigation of the matter. It also engaged cybersecurity experts to assist with the process. On March 19, 2024, the investigation determined that certain files may have been acquired without authorization. After a thorough review of those files, on or about May 8, 2024, certain personal information was identified as being contained within the affected data.

2. Number of Maryland Residents Affected

On June 7, 2024, Local SEIU 1000 notified one (1) Maryland resident of this incident via first class U.S. mail. The affected information for these individuals may have included a name in combination with the individuals' medical information and/or Social Security numbers. 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 SEIU 1000 is implementing additional security measures. It is also offering complimentary credit and identity protection monitoring to all notified individuals.

4. Contact Information

Local SEIU 1000 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 503.459.7707 or shoar@constangy.com, or Jamie Seibert at 816.853.5579 or jseibert@constangy.com.

Regards,



Sean Hoar
Partner and Chair

Enc.: Sample Consumer Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Subject: Notice of Data Security Incident / Notice of Data Breach)>>

Dear <<first_name>> <<last_name>>:

We are writing to inform you of a recent data security incident experienced by the Union of California State Workers dba Local SEIU 1000 ("Local SEIU 1000") headquartered in Sacramento, California, that may have involved some of your information. This letter is to notify you of the incident and inform you about steps you can take to help protect your personal information.

What Happened: On January 18, 2024, Local SEIU 1000 experienced a network disruption and immediately initiated an investigation of the matter. We also engaged cybersecurity experts to assist with the process. On March 19, 2024, the investigation determined that certain files may have been acquired without authorization. After a thorough review of those files, on or about May 8, 2024, some of your information was identified as being contained within the affected data.

What Information Was Involved: The information may have included your <<b2b_text_2 (name, data elements)>>.

What We Are Doing: As soon as Local SEIU 1000 discovered the incident, we took the steps described above and implemented measures to enhance network security and reduce the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation necessary to hold the perpetrators accountable. We are also offering you 12 months of complimentary identity monitoring services through Kroll.

What You Can Do: You can follow the recommendations included with this letter to help protect your information. In addition, you can also activate Kroll's complimentary identity monitoring services.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call <<call center number>> between 6 a.m. to 3:30 p.m. Pacific Time, excluding major US holidays.

The security of the information in our possession is a top priority for Local SEIU 1000. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "William R. Hall". The signature is fluid and cursive, with the first name "William" and last name "Hall" being clearly legible.

William Hall, Chair
Union of California State Workers
dba SEIU Local 1000
P.O. Box 160005
Sacramento, CA 95816

Steps You Can Take to Help 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
marylandattorneygeneral.gov/
1-888-743-0023

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.