



North Los Angeles County Regional Center

Main 818-778-1900 • Fax 818-756-6140 | 9200 Oakdale Avenue #100, Chatsworth, CA 91311 | www.nlacrc.org

January 3, 2025

[Name]

[Address 1]

[Address 2]

[City, State Zip]

Notice of Data Incident

Dear [Name],

I am writing to inform you that North Los Angeles County Regional Center (“NLACRC” or “we”) experienced a data incident in November 2024 (“Incident”) which involved your personal information (“Information”). This letter provides you with information about this Incident and where you can direct any questions. Although we are unaware of any identity theft or fraud in relation to the Incident, as a precaution, we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for twelve (12) months.

What Happened?

On November 28, 2024, we discovered suspicious activity on our systems with indicators consistent with a ransomware event. We immediately began an investigation and took steps to contain the situation. This included notifying federal law enforcement and engaging cybersecurity and privacy professionals to assist.

Currently, the investigation found evidence of unauthorized activity within NLACRC computer systems November 20, 2024, through December 1, 2024, and that an unauthorized actor took a copy of some information before encrypting or encoding certain computer systems to render them inaccessible. Our investigation determined that some of your Information was copied from our systems. While there is currently no evidence of identity theft or fraud in relation to this Incident, your trust is important to us.

What Information Was Involved?

NLACRC may have previously received or collected your Information because you or someone you know provided your Information in order to receive services. Based on the findings of the investigation, the following Information related to you was: [Data Elements].

What We Are Doing.

Upon becoming aware of the Incident, we immediately took steps to further improve the security of our systems and practices. This included enhancing our monitoring processes for increased protection from cybersecurity threats, changing passwords, and strengthening password practices. After determining that an unauthorized actor gained access to our systems, we immediately began analyzing available information to confirm the identities of potentially affected individuals and notify them. We added further technical safeguards to our existing protections and brought systems back online as quickly and securely as possible. We are working diligently to complete our investigation and if we find additional Information about you, we will send you another letter. We continue to work with leading privacy and security firms to aid in our response, and we have reported this Incident to relevant government agencies.

While the investigation is ongoing and to help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twelve (12) months. To start monitoring your personal information, please follow the steps below:

- You must **enroll by** March 31, 2025, at 3:59 pm Pacific Time (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: [insert code].

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this Incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 Monday through Friday 6 am – 6 pm Pacific Time by March 31, 2025. Be prepared to provide engagement number B137509 as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do.

In addition to enrolling in credit monitoring services, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

NLACRC takes the security of personal information seriously and we apologize for any concern this Incident may cause. If you have questions related to credit monitoring services, please contact Experian at the number provided above. If you have any other additional questions, you can contact the toll-free assistance line for our dedicated call center at 855-295-5618, Monday through Friday, from 6:00 am to 6:00 pm Pacific Time (excluding some U.S. national holidays).

Sincerely,

Megan Mitchell

Megan Mitchell, M.S.
Privacy Manager
North Los Angeles County Regional Center

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Protecting Medical Information. If you are concerned about protecting your medical information, 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.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.