[redacted] [redacted]

The Housing Authority
of the City of Los Angeles

December 5, 2025

NOTICE OF DATA BREACH

Dear [redacted],

The Housing Authority of the City of Los Angeles ("HACLA") is providing notice of an incident that may have impacted information you may have provided us. We take the privacy and security of your information seriously and sincerely regret any concern or inconvenience this may cause you.

What Happened?
In October 2024, HACLA identified suspicious activity on its IT systems indicating potential unauthorized access. HACLA immediately implemented its incident response protocols and began an investigation. Independent computer forensic experts were involved to assist with conducting that investigation to determine the scope and extent of the incident. The investigation determined that there had been unauthorized access to HACLA's systems. In January 2025, a third-party vendor was hired to review the potentially impacted data and identify the personal information that was present at the time of the unauthorized access. In July 2025, the investigation determined that personal information was present during the unauthorized access and may have been accessed during the incident. HACLA next worked to find any email addresses associated with potentially impacted individuals in the potentially impacted data and worked to provide those potentially impacted with credit monitoring and restoration services. This process took considerable time to complete. At this time, HACLA has no evidence that any such information has been misused.

What Information Was Involved?
From our review, the following data elements may have been disclosed: Date Of Birth; Social Security Number; Email; Phone Number; Street Address; Financial Account Number ; Diagnosis Or Treatment Or Procedure.

What We Are Doing.
In response to the incident, HACLA has taken decisive steps to strengthen its security practices, including completing the implementation of a new security information management system and continuing to apply vulnerability patches as they become available to prevent similar events in the future. HACLA has also notified the FBI and other law enforcement agencies of this incident.

In addition, although HACLA has no evidence of misuse of information as a result of this incident, HACLA is offering twelve (12) months of credit monitoring and restoration services from IDX at no cost available to anyone who was impacted by this incident.

What You Can Do.
We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-855-202-8327, going to https://app.idx.us/account-creation/protect and using the following Enrollment Code: [redacted]. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is March 5, 2026.

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can

[redacted]

answer questions or concerns you may have regarding protection of your personal information.

For More Information.
If you have questions, please call 1-855-202-8327, Monday through Friday from 6 am - 6 pm Pacific Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Recommended Steps to Help Protect Your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8258. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-888-378-4329	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft , 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

[redacted] [redacted]

This email was sent by: IDX to [redacted]
4145 SW Watson Ave #400, Beaverton, OR 97005 US
Privacy Policy

[redacted]