EASTERN LOS ANGELES REGIONAL CENTER

1000 S. Fremont Ave. • P.O. Box 7916 • Alhambra, CA 91802-7916 • (626) 299-4700 • FAX (626) 281-1163

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<b2b_text_1(Care-of Info)>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>>:

We are writing to inform you of a data security incident that may have involved your information as described below.

Eastern Los Angeles Regional Center (ELARC) takes the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was subject to actual or attempted misuse during this incident, it is crucial that we be as supportive and transparent as possible. That is why we are writing to inform you about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened:

On July 15, 2021, ELARC learned of suspicious activity related to one employee email account. Upon discovery, ELARC took swift action to secure its email system and network. ELARC also immediately launched an internal investigation and engaged leading, independent cybersecurity specialists. Based on this investigation, on August 11, 2021 ELARC confirmed that one employee email account was subject to unauthorized access for a limited period of time on July 15, 2021. Upon discovery, we moved quickly to notify all active consumers in an abundance of caution while we further investigated the potential scope of at risk data. This included a thorough programmatic and manual review of the entire mailbox contents in order to identify what information was present and to whom it belonged. On October 6, 2021, this review was completed and we immediately worked to review our internal files for up-to-date address information to provide individuals with notification.

While we have no reason to believe that any information within the affected email account was subject to actual or attempted misuse during this incident, we are providing this notification to you out of an abundance of caution and so that you may monitor your information and take advantage of the complimentary resources being offered to you.

You may have received a similar letter from ELARC in September or October of this year. Please note that this letter provides additional information related to the same incident and is not to notify you of a separate incident.

What Information Was Involved:

The types of information present within the affected mailbox included your first and last name in combination with the following data elements: <<b2b_text_1(Data Elements)>>.

What We Are Doing:

We have taken every step necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took the steps described above. We have also implemented additional technical safeguards to further enhance the security of information in our possession and prevent similar incidents from happening in the future. Additionally, we are offering you complimentary identity monitoring services.

In addition, we have arranged for you to activate, at no cost to you, an online identity monitoring service for 12 months provided by Kroll. Due to privacy laws, we cannot activate you directly. Additional information regarding how to activate the complimentary identity monitoring service is enclosed. Please note that if you activated these services pursuant to an earlier letter, there is no need to activate again.

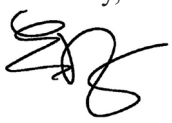
What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your accounts and explanation of benefits statements to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information:

ELARC has established a dedicated assistance line to address any questions you may have which can be reached at 1-855-651-2690, Monday through Friday, 6 a.m. to 3:30 p.m. Pacific Time, excluding major US holidays. You may also contact ELARC by mail at P.O. Box 7916, Alhambra, CA 91802. The security of our consumers' information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,



Edith Hernandez-Daniels
Chief of Consumer Services

STEPS YOU CAN TAKE TO HELP PROTECT INFORMATION

Activate 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>>**

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 will 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.

You can sign up for the online identity monitoring service anytime between now and **<<b2b_text_6(Activation Deadline)>>**. Due to privacy laws, we cannot activate you directly. Activating this service will not affect your credit score. You must be over age 18 with a credit file activate these services.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;

5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.