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

Enrollment Code: <<XXXXXXXX>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

January 24, 2025

NOTICE OF DATA SECURITY INCIDENT

Dear <<First Name>> <<Last Name>>,

Jack Doheny Company is writing to inform you of a recent data security incident that may have involved your personal information. While there is currently no indication that any identity theft has occurred as a result of this incident, some of your personal information was included on the systems that were impacted by this incident, so we want to let you know what happened, what is being done to address it, and the complimentary identity monitoring services we are offering.

What Happened?

Like many other companies in recent years, we were the unfortunate victim of a cybersecurity incident involving unauthorized access to our systems. Upon discovery of unusual network activity, we immediately engaged our internal security team, took steps to secure our network environment, launched an investigation with help from outside cybersecurity experts, and notified law enforcement. Although it was initially determined that no employee personal data had been taken from the network as a result of the incident, the investigation subsequently identified in early December 2024 that an unauthorized third party obtained a subset of our files in approximately late February 2024.

Although we have not conclusively determined whose information may have been contained in the affected files, we are providing this notification out of an abundance of caution. We are not aware of any evidence to date that any personal information associated with the incident has been used for identity theft.

What Information Was Involved?

To date, we have been unable to determine with certainty what personal information was accessed or acquired as a result of this incident. However, the following types of employee personal information were located on the systems that were compromised as a result of the incident: full legal name, date of birth, social security number, tax information, payroll statements, driver's license or other government identification number, bank or financial information, and other personnel-related information.

What We Are Doing.

We deeply regret the inconvenience that this incident may cause you. As described above, we took steps to secure our systems, launched an investigation immediately after discovering the incident, and notified law enforcement authorities. To help minimize the likelihood of similar occurrences in the future, we will continue to monitor our systems for any suspicious activity, and we have implemented additional measures designed to enhance the security of our network, systems, and data. We will continue to evaluate ways to further enhance the security of our systems.

As an added precaution and to relieve concerns, we are offering you complimentary credit monitoring and identity protection services through IDX, the data security incident and recovery services expert. IDX identity protection services include: 2 years of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do.

Although there is no evidence that your information has been misused, we encourage you to contact IDX with any questions and to enroll in the complimentary credit monitoring and identity protection services by calling 1-833-903-3648, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 AM – 8:00 PM Central Standard Time. Please note the deadline to enroll is April 24, 2025. The enclosed reference guide includes additional information on general steps you can take to monitor and protect your personal information.

We encourage you to remain vigilant against incidents of identity theft and fraud, such as by regularly reviewing your account statements with all of your financial institutions. You may also choose to monitor your credit reports. The resources guide enclosed in this letter describes additional steps you can take and provides contact details for the Federal Trade Commission and credit reporting agencies, as well as information on how to place fraud alerts and security freezes.

For More Information.

The protection of your information is important to us, as is addressing this incident fully and providing you with the information and assistance you may need. You will find detailed instructions for enrollment and additional information on general steps you can take to monitor and protect your personal information in the enclosed reference guide. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-903-3648 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Jack Doheny Company

Recommended Steps to Help Protect your Information

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. 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 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file and obtain 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, your state Attorney General, or the Federal Trade Commission.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying 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.

6. Place Fraud Alerts with the three credit bureaus. As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on your credit file. Upon seeing a fraud alert display on your credit file, 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, which is a fraud alert lasting 7 years. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.

7. You can obtain additional information regarding identity theft, fraud alerts, credit freezes, and steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You may contact the Federal Trade Commission as follows: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

New York residents: New York residents may obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.