Return Mail Processing Center
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: October 1, 2025

To Enroll, Scan the QR Code Below:

SCAN ME

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

July 1, 2025

Re: Notice of Data Security <<Variable Data 2>>

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

We are writing to inform you of a data security incident that involved your personal information. Idealab is a technology incubator and received your information in conjunction with related services. You may be receiving this letter because you are a current or former employee of an entity that contracted with Idealab for employee support services, a dependent of one, or a former contractor. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On or around October 7, 2024, Idealab became aware of unusual activity in its digital network. We immediately took steps to secure our network and engaged cybersecurity experts to conduct an investigation. The investigation determined that an unknown actor acquired certain data without authorization on or about October 4, 2024. We then engaged a third-party vendor to conduct a comprehensive review of the affected data to determine whether personal information may have been involved. Based on that review, on June 26, 2025, Idealab confirmed the scope of the impact and secured information sufficient to effectuate notice. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The data involved included your name in combination with your <<Variable Data 1>>.

What We Are Doing: In addition to the steps described above, we implemented additional security measures to further protect our network and minimize the risk of future incidents. We also reported this incident to the Federal Bureau of Investigation.

We are also offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include 24 months of credit[1] and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is October 1, 2025. With this protection, IDX will help to resolve issues if your identity is compromised.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through IDX by contacting 1-800-939-

[1] To receive credit monitoring 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.

4170 or going to https://app.idx.us/account-creation/protect and using the enrollment code above. Please note the deadline to enroll is October 1, 2025.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays). IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Sincerely,

Idealab
130 W. Union Street
Pasadena, CA 91103

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps

the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

California: California Attorney General can be reached at: 1300 I Street, Sacramento, CA 95814; 800-952-5225; www.oag.ca.gov/privacy

Iowa: Iowa Attorney General can be reached at: 1305 E. Walnut St., Des Moines, IA 50319; 888-777-4590; www.iowaattorneygeneral.gov

Kentucky: Kentucky Attorney General can be reached at: 700 Capitol Avenue, Suite 118, Frankfort, KY 40604; 502-696-5300; www.ag.ky.gov

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; consumer@oag.state.md.us or IDTheft@oag.state.md.us or www.marylandattorneygeneral.gov/Pages/CPD

Oregon: Oregon Attorney General can be reached at: 1162 Court St., NE, Salem, OR 97301; 877-877-9392; www.doj.state.or.us/consumer-protection

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov/protectingconsumers/

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 1-401-274-4400. The total number of Rhode Island residents receiving notification of this incident is 3.

Washington D.C.: Washington D.C. Attorney General can be reached at: 400 S 6th Street, NW Washington, DC 20001 oag.dc.gov/consumer-protection 1-202-727-3400