National Lead for America, Inc
c/o Cyberscout
P.O. Box 3923
Syracuse, NY 13220

[redacted]

To enroll, please visit:

https://secure.identityforce.com/benefit/leadforamerica
Enrollment Code: [redacted]

November 21, 2022

Notice of Data Breach

Dear [redacted]

What Happened

This letter is to inform you that Lead for America ("LFA") discovered a data security incident affecting one of our employee's email accounts.

Upon discovery of this incident, we worked with third-party cybersecurity experts to respond to the incident and conduct an investigation. We also immediately informed law enforcement and will cooperate in any investigation they may pursue.

Based on our investigation to-date, an unknown third-party compromised an employee's email credentials and accessed that employee's email without authorization. This compromise was leveraged by the threat actor to access certain LFA shared files. Shortly after the compromise, the unauthorized access was stopped, and then the employee account was secured.

At this time, this incident appears to be financially motivated, and not related to the theft or misuse of your personal data. We do not have any evidence of access to your specific data, however we have determined that the potentially compromised files contained information about you. We are sending you this notification and set of resources to inform you of this incident and continue our commitment to protecting your data.

What Information Was Involved

Files subject to unauthorized access contained certain personal information for LFA employees, fellows, and related individuals.

The information about you contained in these files includes the following: full name; social security number; date of birth; and payroll information including account and routing number.

What We Are Doing

We take the security of your personal data very seriously. We are taking steps to investigate this incident and enhance our security program to help prevent similar incidents from happening in the future, including providing additional training to our workforce around phishing campaigns and security best practices, reviewing and updating our data retention and handling practices, and considering additional tools and software to further harden our environment.

In addition, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to contact Cyberscout with any questions by calling 1-833-519-0947 and supply the fraud specialist with your unique code listed below. Cyberscout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Again, at this time, there is no indication that your information has been misused. However, we encourage you to take full advantage of this service. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding the protection of your personal information.

For More Information

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the Activation Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call Cyberscout at 1-833-519-0947 between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays, for assistance or for any additional questions you may have.

Sincerely,

Joe Nail
Chief Executive Officer
Lead for America

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to **https://secure.identityforce.com/benefit/leadforamerica** and follow the instructions for enrollment. When prompted please provide the following unique code to receive services: [redacted]**.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Activate the credit monitoring provided as part of your Cyberscout 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, Cyberscout will be able to provide guidance for you.

3. Telephone. Contact Cyberscout at 1-833-519-0947 between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays, 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 Cyberscout identity protection, notify Cyberscout of them immediately by calling or by logging into the Cyberscout 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 the customer care team who will assist you in determining 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 Cyberscout Restoration agent who will work with you to identify, stop and reverse the damage quickly.

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.

5. 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. 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:

Equifax Fraud Reporting	**Experian Fraud Reporting**	**TransUnion Fraud Reporting**
1-866-349-5191	**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 19022-2000**
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.

6. 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.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

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