NATIONAL RIGHT TO WORK LEGAL DEFENSE FOUNDATION, INC.
8001 BRADDOCK ROAD, SUITE 600, SPRINGFIELD, VIRGINIA 22160 • (703) 321-8510

William L. Messenger
Vice President & Legal Director (admitted in VA)

Fax (703) 321-9319
E-mail wlm@nrtw.org

January 17, 2024

<<First Name>> <<Last Name>>
<<Address>>
<<City>>, <<State>> <<Zip>>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Please read this letter in its entirety.

We are writing to notify you of a recent data security incident that may affect the security of some of your sensitive personal information.

Although we have no indication of identity theft or fraud in relation to this event, we take the protection of your information very seriously and are contacting you directly to explain the circumstances, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On Sunday, November 12, 2023, we became aware of a ransomware attack on our computer network. Upon discovering the incident, we promptly shut down our network to halt the progress of the attack and lock down our network, and we retained outside cyber security experts to investigate the incident. The investigation revealed that an unknown third party exploited a vulnerability in a public-facing forum and deployed tools to gain remote access to our network. From there, the threat actor deployed ransomware and encrypted systems, as well as files on those systems. Through the investigation, we determined that the threat actor exfiltrated certain limited data.

It appears that this cyber attack is a random attack by an unknown threat actor. We have notified and are working with law enforcement on this incident. These actions have not delayed this notice.

Through our investigation, we have been able to determine the threat actor accessed or acquired some documents that contain your personal data.

What Information Was Involved? Our investigation has shown the threat actors have obtained the following personal data associated with you: first and last name and social security number.

The Foundation's legal department has this information in its archived case records, which contain documents and information obtained legally during the course of a legal aid case.

What We Are Doing. Upon discovering the threat actor's exploitation, our IT department promptly shut down our network and began working closely with cybersecurity experts to

investigate the incident and to put in place security measures to strengthen our network against similar incidents in the future. We also took steps to analyze the potentially affected data to determine the scope of the incident and what data, if any, the threat actors may have accessed or acquired. In conducting the forensic investigation, we confirmed the threat actors have not regained access to our systems. Further, we are evaluating our procedures with respect to data that we maintain on our servers, are reviewing security policies for any potential updates, and are revisiting our cybersecurity standards.

In response to the incident, we are providing you with access to **Triple Bureau Credit Monitoring/TransUnion Credit Report** services at no charge. These services provide you with alerts for 18 months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. 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 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.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/nrtw and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<CODE HERE>>**. 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.

What You Can Do. We want to make sure you are aware of steps you may take to guard against potential identity theft or fraud. We strongly urge you to review the enclosed *Steps You Can Take to Protect Personal Information* for information about what you can do to safeguard against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to us, local law enforcement, or your state's attorney general.

For More Information. If you have further questions or concerns about this incident, you may call 1-800-405-6108 Monday through Friday from 8:00 AM to 8:00 PM Eastern Time (excluding U.S. holidays). Representatives are available for 64 days from the date of this letter, and please supply the fraud specialist with your unique code listed above when you call.

Sincerely,

William L. Messenger

Enclosure

For residents of District of Columbia, Maryland, and North Carolina:

You can obtain information from the District of Columbia, Maryland, and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General
400 6th Street NW
Washington, DC 20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
https://ncdoj.gov/

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

***Massachusetts*:** You have the right to obtain or file a police report.

For residents of all states:

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft.

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies listed below. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts, free of charge, by contacting any of the three credit bureaus listed below. 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency listed below.

In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you may need to provide your full name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/education/credit/report/articles/-/learn/how-to-get-your-free-credit-report/	https://www.experian.com/consumer-products/free-credit-report.html	https://www.transunion.com/annual-credit-report
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Consumer Fraud Division, P.O. Box 105069, Atlanta, GA 30348 https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf	Experian Fraud Center, P.O. Box 9554, Allen, TX 75013 www.experian.com/fraud/center.html	TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016 www.transunion.com/fraud-victim-resource/place-fraud-alert
Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348 www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 http://www.experian.com/freeze/center.html	TransUnion Security Freeze, P.O. Box 160, Woodlyn, PA 19094 www.transunion.com/credit-freeze

Additional Information: The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general.