[CLIENT LOGO]
<<Return Address>>
<<City>>, <<State>> <<ZIP>>

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

<DATE>

NOTICE OF DATA SECURITY INCIDENT

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

Health Resources in Action, Inc. ("HRIA") recently experienced a data security incident that may have impacted some of your personal information. We take the privacy and security your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about the steps you can take to protect your information, and resources we are making available to help you. These services are provided at no cost to you.

What Happened?

On April 24, 2024, we discovered suspicious activity associated with our email environment. We immediately implemented our incident response protocols, took steps to secure the email environment, and engaged independent computer forensic experts to assist with an investigation. The investigation found that there was unauthorized access to a single email account and a few SharePoint files between March 29, 2024, and April 24, 2024. We then reviewed the emails in the account and files in SharePoint to identify any personal information present during the unauthorized access. Our investigation determined that your personal information was present in one of the SharePoint files that may have been viewed by the unauthorized user. While there is no evidence that your information has been misused, we wanted to make you aware of this incident out of an abundance of caution.

What Information Was Involved?

It appears that your legal name, address, Social Security number, driver's license number, and date of birth provided to HRIA in connection with a background check may have been affected.

What We Are Doing:

Immediately after identifying the incident, changed passwords to email accounts, reset the multi-factor authentication, and all HRIA staff are completing their annual data security training. In addition, although there has been no evidence your information was misused, we previously offered you identity theft protection services through Experian IdentityWorks for twenty-four (24) months.

What You Can Do:

We have provided you with a code to access 24 months of complimentary credit monitoring and identity restoration services through Experian. You shared with us that you have enrolled in the service.

This letter also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information:

If you have questions, please contact HRIA at [redacted] Protecting your information is important to us, and we sincerely apologize for any concern this event may cause you.

Sincerely,

Health Resources in Action, Inc.

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided in the previous correspondence you received.

2. Activate the credit monitoring provided as part of your Experian IdentityWorks 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, Experian will be able to assist you.

3. Telephone. Contact Experian at [redacted]f you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online.

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.

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 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	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 following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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.