National Community Reinvestment Coalition
202 628-8866 | www.ncrc.org
740 15th Street, NW
Washington, DC 20005



October 11, 2024

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Sent via email: idtheft@oag.state.md.us

**Re: Security Breach Notification**

Dear Sir or Madam:

In accordance with Maryland's data breach notification requirements, National Community Reinvestment Coalition Inc. ("NCRC") is providing this notice regarding a recent data security incident. The notice includes (i) name and contact information of the reporting entity; (ii) name and contact information of the entity that experienced the breach; (iii) the nature of the breach of the security system; (iv) the types of personal information compromised by the breach; (v) the number of Maryland residents affected; (vi) cause of the breach; (vii) remedial action taken; (viii) date and time frame of the breach; and (ix) any knowledge of foreign country involvement.

**Name and Contact Information of the Reporting Entity**

| | |
|---|---|
| Name of Entity/ Company: | National Community Reinvestment Coalition Inc. |
| Name of Contact Person: | Rosemary Ramirez |
| Title: | Corporate Counsel & Director of Compliance |
| Contact Information: | 202.464.2731<br>rramirez@ncrc.org |

**Name and Contact Information of the Entity That Experienced the Breach**

| | |
|---|---|
| Name of Entity/ Company: | Human Resource Technologies, Inc. (“HRTec”) |
| Address: | 5400 Shawnee Road #201<br>Alexandria, VA 22312 |
| Phone Number: | 703.719.0778 |
| Email: | UNKNOWN |

**Nature & Cause of the Breach**

On July 29, 2024, Growth Builders, LLC (“Growth”) notified NCRC that a third-party vendor, Human Resources Technologies, Inc. (“HRTec”), experienced a data security incident. NCRC does not have any knowledge to suggest the involvement of a foreign country.

Relationship Between Entitles. Growth, an NCRC affiliate organization, hired HRTec to provide IT services.

Date & Timeframe of the Breach. On or about December 5, 2023, Growth identified suspicious activity involving certain services provided by HRTec. At that point, HRTec advised Growth that the issue was resolved. Yet, on January 5, 2024, Growth began receiving communications from the threat actor(s) directly and the organization recognized that they were victims of a cyber-attack due to a shared connection with HRTec. HRTec was the threat actor’s original target.

Remedial Actions by Growth. Upon discovery, Growth took immediate action to address and investigate the incident which included engaging an independent third-party forensic specialist to determine the nature and scope of the incident. Growth completed its review on May 30, 2024.

Types of Personal Information Compromised. On July 29, 2024, Growth notified NCRC that the forensic specialist identified that a 2019 employee census data containing information related to certain NCRC employees participating in the shared NCRC and NCRC Development Corporation 401K may have been impacted by the breach. That document included the following Personal Identifiable Information (“PII”):

- Names
- Addresses
- Social Security Numbers
- 401k Balance Amount

Number of Maryland Residents Affected. A total of forty (40) Maryland residents were affected.

Remedial Actions by NCRC. On August 5, 2024, NCRC promptly provided notice via email to all current staff that were affected by the data security breach because NCRC had access to current staff email addresses while NCRC did not have email information for prior employees affected.

On September 20, 2024, NCRC mailed proper notices to all individuals affected. These notices included information on how to access free 24-month credit monitoring services. I am attaching a copy of the notice provided in the email for your reference.

NCRC understands the seriousness of this matter and is committed to ensuring the protection of the personal information of our employees. If you require any further information or documentation, please do not hesitate to contact me.

Sincerely,

Rosemary Ramirez
Corporate Counsel & Director of Compliance
202.464.2731
rramirez@ncrc.org

NCRC
National Community Reinvestment Coalition

202 628-8866 | www.ncrc.org
740 15th Street, NW
Washington, DC 20005



[Name]
[ADDRESS]

**Re: Notice of Third-Party Vendor Data Breach**

Dear [NAME],

We are writing to inform you of a third-party vendor's data security incident in which your sensitive personal information may have been accessed by an unauthorized third party. Notably, we have no evidence of any misuse of information at this time.

This notice provides information concerning the incident and the services we are offering at no charge to help you protect yourself.

**What Happened?**

On July 29, 2024, NCRC was notified that a third-party IT services provider, Human Resources Technologies, Inc. ("HRTec"), experienced a data security incident.

On or about December 5, 2023, an affiliate organization began receiving communications from the threat actor(s) directly and the organization recognized that they were victims of a cyber-attack due to a shared connection with HRTec. HRTec was the threat actor's original target. Upon discovery, the affiliate organization took immediate action to address and investigate the incident which included engaging an independent third-party forensic specialist to determine the nature and scope of the incident.

**What Information Was Involved?**

The investigation indicated that Personal Identifiable Information ("PII") related to certain NCRC employees participating in the shared NCRC and

NCRC Development Corporation 401K plan may have been potentially impacted.  PII includes your name, address, age, and social security number.  In addition, the information of your 401k balance in 2019.

**What Is NCRC Doing?**

NCRC promptly took a series of steps to remedy the situation including providing proper notice and contacting law enforcement.  Although this was a third-party security breach, NCRC continues to work with outside forensics and cybersecurity experts to identify how to further secure our systems.

More importantly, there is no evidence at this time that your information has been misused for identity theft or fraud because of this incident. To help protect your identity, we are offering you 24 months of identify protection services and credit monitoring from a leading identity monitoring services company at no charge to you.  These services help detect possible misuse of your PII and provides you with identify protection support focused on identification and resolution of identity theft. For instruction on completing the enrollment process for these complimentary protection services, please refer to the instructions enclosed with this notice.

**What can you do?**

In addition to the complimentary identity protection services and credit monitoring we are providing you; we want to make you aware of further steps that you can take as a precaution.  Please review the 'Additional Information' enclosed for your convenience.

**For More Information**

If you have any further questions regarding this incident, please contact me via email (rramirez@ncrc.org) or via phone (202.464.2731).  You may also contact NCRC's Chief Operating Officer Gregory Dyson at gdyson@ncrc.org.

Sincerely,

Rosemary Ramirez
Corporate Counsel & Director of Compliance

## Enrolling in Credit Monitoring Services at No Charge

**COMPLIMENTARY SERVICE OFFER:** At our expense, Aura would like to offer you a free 24-month subscription to Identity Defense Total, a credit monitoring and identity theft protection service. Identity Defense Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations.

IDENTITY DEFENSE TOTAL features include:

- Dark Web Monitoring
- High Risk Transaction Monitoring
- Customer Support & Victim Assistance
- 3-Bureau Credit Monitoring
- $1 Million Identity Theft Insurance*
- Monthly Credit Score
- Identity & Authentication Alerts
- Security Freeze Capability

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you wish to take advantage of this monitoring service, you must enroll by **November 30, 2024.**

ENROLLMENT PROCEDURE: To activate this coverage please visit the Web site listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

**Web Site: app.identitydefense.com/enrollment/activate/ncrc**

**Activation Code: [Activation Code]**

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address
- Activation Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We urge you to enroll today

## Additional Information

- **Review Accounts and Credit Reports.** You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annual creditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

  *You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC").* You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft. The FTC can be reached at: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

  **For Washington, D.C. Residents:** You may obtain information about preventing and avoiding identity theft from the Washington D.C. Attorney General's Office: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, (202) 727-3400. https://oag.dc.gov/consumer-protection.

  **For Maryland Residents:** You may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1(888) 743-0023.

  **For Virginia Residents:** You may obtain information about preventing and avoiding identity theft from the Virginia Office of the Attorney General, 202 North Ninth Street, Richmond, VA 23219, 804-786-2071.

- **Security Freezes and Fraud Alerts.** You have a right to place a security freeze on your credit report at no cost, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit mortgage, or any other account involving the extension of credit. You may request that a freeze be placed on your credit report by calling the numbers of the credit reporting agencies specified below by certified mail, overnight mail or regular stamped mail, or by visiting the website addresses of the credit reporting agencies below.

  A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

  As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on you credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the following national credit reporting agencies:

**Equifax (www.Equifax.com)**
GENERAL CONTACT:
PO BOX 740241, Atlanta, GA 30374
800.685.1111
Fraud Alerts and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

**Experian (www.experian.com )**
GENERAL CONTACT:
P.O. Box 2104, Allen, TX 75013
888.397.3742

Fraud Alerts and Security Freezes:
P.O. Box 9556, Allen, TX 75013
**TransUnion (www.transunion.com)**
GENERAL CONTACT, FRAUD ALERTS & SECURITY FREEZES:
P.O. Box 2000, Chester, PA 19022
800.916.8800

## Additional Information

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111
General Contact: P.O. Box 740241, Atlanta, GA 30374
Fraud Alerts and Security Freezes: P.O. Box 740256, Atlanta, GA 30374

Experian: experian.com/help or 1-888-397-3742
General Contact: P.O. Box 2104, Allen, TX 75013
Fraud Alerts and Security Freezes: P.O. Box 9556, Allen, TX 75013

TransUnion: transunion.com/credit-help or 1-888-909-8872
General Contact, Fraud Alerts and Security Freezes: P.O. Box 2000, Chester, PA 19022

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

Additional information is available from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.