CICGROUP.COM

TO: Affected Individuals

FROM: CIC Group, Inc.

DATE: April 21, 2023

NOTICE OF DATA BREACH

CIC Group, Inc. and its business units ("we") value and respect the privacy of your information, which is why we are writing to inform you of a data security incident that has occurred that may involve your personal information. We recommend that you closely review the information provided in this letter for some steps that you should take to help protect yourself against potential misuse of your personal information.

WHAT HAPPENED?

On March 28, 2023, we became aware that most of our computer systems had become subject to a ransomware attack by an unknown threat actor. Once we became aware, we immediately disabled the affected systems and began a thorough investigation into the incident. That same day, we also moved swiftly to engage a forensic investigations service provider to investigate the incident. We are working to return normal operations for CIC Group and its subsidiaries as quickly as possible.

The ransomware attack led to encryption and/or destruction of data on the affected systems. Since the data has been either encrypted or destroyed, we have not been able to fully determine the scope of the attack. On April 13, 2023, the threat actor provided information that leads us to believe the personal information of certain individuals was part of the attack and taken from our systems during the attack. Such unauthorized acquisition by the threat actor would constitute a breach under applicable data breach notification laws. At this time, we do not know the full extent of the personal information that was subject to the attack. However, out of the utmost of caution, we are sending this notice to those individuals whose personal information we reasonably believe could have been subject to the attack.

We value your privacy and deeply regret that this incident occurred.

WHAT INFORMATION WAS INVOLVED?

The personal information acquired in the attack potentially included your first and last name, address, email address, date of birth, phone number, social security number, passport information, tax ID information, and benefit information.

WHAT WE ARE DOING

As soon as we became aware of the attack, we engaged third-party service providers to help us investigate the incident and its causes. With their help, we are working to restore existing, or implement new, systems with additional security measures designed to better help us avoid the recurrence of a similar attack. We also hired a third-party service provider to monitor for any disclosures, or any other sign of unlawful behavior, with respect to your personal information. None has been found as of the date of this notice, but we will certainly notify you if any such activity arises.

Further, we informed the appropriate law enforcement agencies and are working with law enforcement to ensure the incident is properly addressed. This notice was not delayed as a result of a law enforcement investigation.

WHAT YOU CAN DO

Please also review the Steps You Can Take to Further Protect Your Information section below for further information on steps you can take to protect your information and how to receive free credit monitoring/identity protection services for 24 months.

FOR MORE INFORMATION

We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling in the credit monitoring services online, please call **[ENTER TOLL FREE NUMBER]** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **[B_____]**. You may also contact us at CIC Group, Inc., 1509 Ocello Drive, St. Louis, MO 63026.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

You should remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov, call 1-877-ID-THEFT (877-438-4338), or mail the compliant to Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

You should obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. You can do this by:

1. Visiting http://www.annualcreditreport.com;
2. Calling toll-free 877-322-8228, or
3. 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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action.

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
(877) 322-8228
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Place a Fraud Alert on Your Credit Report

You should place a fraud alert on your credit report. An initial 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. 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.

Credit Monitoring and Identity Protection

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by **July 31, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: **[Activation Code]**

If 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, please contact Experian's customer care team at **[ENTER TOLL FREE NUMBER]** by **July 31, 2023**. Be prepared to provide engagement number **[B_____]** as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding Your 24-Month Experian IdentityWorks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[*]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[†]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

---

[*] Offline members will be eligible to call for additional reports quarterly after enrolling.

[†] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/501a-identity-theft-a-recovery-plan_2018.pdf.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/ default.aspx or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400.

North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

OTHER IMPORTANT INFORMATION

Security Freeze

Under 15 U.S.C. Section 1681c-1 and certain state laws, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. Using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

Your Rights Under the Federal Fair Credit Reporting Act

You have rights pursuant to the Fair Credit Reporting Act, such as, the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting by visiting www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W. Washington, DC 20552.