ROGERS Rg GROUP

May 11, 2022

Notice of Cyber Incident

Rogers Group ("Rogers") is posting this statement on its website as a precautionary measure and as part of our commitment to our employees' privacy. Rogers takes its employees' privacy seriously; it is important to us that both employees and the community that we serve are aware of a recent cyber incident at Rogers' Michigan location, which potentially involves personal information, including limited healthcare information, about our employees and some of their dependents.

On approximately December 20, 2021, our IT staff discovered that an unauthorized party gained access to one of our servers. During the period of time that the threat actors had access, malware was launched, blocking our access and encrypting certain data on the impacted systems. Upon learning of this incident, our management team immediately engaged a cybersecurity incident response and digital forensic firm to investigate the matter, assist in the decryption of impacted data, and review the content of any data that may have been accessed without authorization. This investigation continues, but we have sufficient initial indications to provide this notice to the current and former employees who may have been impacted by this incident.

At this time, we believe approximately 582 documents from the HR Department were accessed, potentially affecting our employees and, in some instances, their dependents. Among the information that has been identified in recent days, is individual health insurance information, such as names, insurance contract information and numbers, claims payments, and dates of service. Social security numbers and a small number of expired credit card numbers also may have been accessed. To date, analysis of the impacted data has determined that only a small percentage of documents (less than 0.2% or approximately 70 documents) contained any medical information, which largely was related to workers' disability claims and requests for leave under FMLA. Current analysis shows that only 77 individuals' health information related to FSA claims was impacted, comprised largely of dental and vision claims, office visits and vaccines. With the data analysis investigation still on-going, once it is complete, we will have a full understanding of the impacted data, and if any other protected health information ("PHI") concerning our employees may have been accessed. We will update this notice if we have any more information to share.

Given the nature of the documents and out of an abundance of caution, we are notifying those current and former employees who may have been impacted by this incident of the possibility that some of their PHI may have been accessed by these unknown, unauthorized threat actors. Because we may not have current physical mailing addresses for some former employees, we have posted this website notice. For others, we are in the process of mailing letters to describe the immediate steps (as described below) that they can take to protect themselves from any potential misuse of their information.

WHAT YOU SHOULD DO

Rogers recommends that you remain vigilant and consider taking one or more of the following steps to protect your protected health information or personal information:

- Contact the nationwide credit-reporting agencies as soon as possible to add a ***fraud alert*** statement to your credit file at all three-national credit-reporting agencies listed below.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months;
- Receive a free copy of your credit report by going to www.annualcreditreport.com;

ROGERS Rg GROUP

- Pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase;
- Review all your bank account statements frequently for checks, purchases, or deductions not made by you; and
- If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC.

We also recommend that you regularly review statements from your accounts (i.e., account statements and Explanations of Benefits ("EOB")) 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.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase additional copies of your credit report by contacting one or more of the three nationwide consumer reporting agencies listed below.

- **Equifax:** P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
- **Experian:** P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
- **TransUnion:** P.O. Box 1000, Chester, PA 19022, 1-800-888-4213 www.transunion.com

When you receive your credit reports, account statements and EOBs, review them carefully. Look for accounts or creditor inquiries, transactions or services that you did not initiate or do not recognize. Look for information that may not be accurate, such as home address and Social Security Number. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report, the company issuing the account statement, your provider rendering services, or the insurance company issuing your EOB.

In addition, we will provide Credit Monitoring for one year at our cost through Experian's IdentityWorks. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: August 31, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: **CRMF998ELY**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 559-2449** by August 31, 2022. Be prepared to provide engagement number: **B052294** as proof of eligibility for the identity restoration services by Experian.

We take the protection of your personal information seriously and took steps with the help of our cyber incident response/digital forensic team to prevent a similar occurrence. Our workforce has changed passwords, implemented multi-factor authentication (requiring multiple ways to access an account) and offered additional training to our workforce in safeguards against phishing attempts.

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (833) 559-2449, Monday-Friday, 8am to 8pm CT and Saturday-Sunday, 10am to 7pm CT (excluding major US holidays).

We sincerely apologize to you and all our clients for concern caused by this incident.

Sincerely,

Rogers Group, Inc.