18498

NOTICE OF DATA BREACH

Dear [Insert Name]:

We want to make you aware of an IT security incident that may impact you as a former employee of a Global Growth affiliated company. On or around December 1, 2020, a hacker gained access to the e-mail account of a Human Resources team member, which, due to the nature of this employee's job, contained sensitive employee personal information. We take this IT security incident very seriously, and we have already taken, and will continue to take, measures to protect you and to harden our systems to better prevent incidents like this in the future.

PLEASE READ THIS NOTICE CAREFULLY AS IT CONTAINS INFORMATION YOU NEED TO PROTECT YOU AND YOUR FAMILY.

If, after reviewing this information, you have any questions, reach out to [include contact person and email/ telephone].

What Happened?

On or around December 1, 2020, an unknown hacker(s) gained access to the email account of an employee in the Global Growth Corporate Human Resources department. We discovered the compromise on December 1, 2020 and immediately took measures to terminate the hacker's access and determine what harm may have occurred.

Our internal and external incident response teams have analyzed forensic evidence left by the hacker to understand the impact of the attack and to identify any personal information that may have been exposed or acquired. As a part of these efforts, which are ongoing, we found evidence that the hacker may have downloaded the sensitive employee personal information described below.

We continue to monitor system logs for alerts and unusual activity in our e-mail system, and we are improving our internal security protocols to detect and avoid similar attacks in the future. For example, we are implementing multi-factor authentication to increase the security of our password-protected systems.

What Information Was Involved?

This incident involved the personal information of some current and former employees and their dependents, including:

- Names
- Dates of Birth
- Addresses
- Phone Numbers

- Email Addresses
- Social Security Numbers/Social Insurance Numbers
- Bank Account Numbers and Routing Numbers
- Driver's License Numbers
- Passport Numbers
- Voter Registration Numbers
- Health Insurance Policy Numbers
- Dental and Vision Insurance Policy Numbers
- Life and Disability Insurance Policy Numbers
- Medical History
- Medical Conditions, Diagnosis Codes and Treatment Details
- Other potentially sensitive information that employees voluntarily provided to HR over the past year

While this investigation proceeds, you may want to take precautions to protect your personal and financial interests.

Steps to Take

We recommend that you 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Never provide personal information in response to electronic communications regarding security breaches, including this one.

Identity Theft Prevention Services

Global Growth is committed to ensuring the protection of its current and former employees and their families. Therefore, as a further protection against potential identity theft, Global Growth has contracted with Identity Force to provide **FREE** personal security protection for all impacted current or former employees whose information was exposed or acquired during the attack and any named beneficiaries who also may have been impacted. Specifically, impacted individuals are entitled to FREE Identity Force identity theft protection and credit monitoring. These services include:

- **Identity Monitoring** – Continuously scours thousands of websites, chat rooms, blogs, and other data sources to detect illegal trading and selling of your personal information. Scans

for your personal information, including social security number, phone number, email addresses, bank account and routing numbers, credit and debit card numbers, driver's license, mother's maiden name and medical identification numbers.

- **Advanced Fraud Monitoring** – Delivers virtually real time alerts when lenders, such as banks, auto dealers, mortgage companies and government agencies, request a copy of your credit report. Early notification helps you stop fraudulent attempts to open a new account or increase a line of credit. Any credit activity can hurt your credit score.
- **Identity Restoration Specialist** – Complete, comprehensive recovery services from Certified Protection Experts available 24/7. Specialists do not just assist you with identity restoration; they save you hundreds of hours by completing the paperwork, making the calls, and doing the heavy lifting to make sure your identity is restored.
- **Identity Theft Insurance** ($1M) – Recover out-of-pocket expenses and lost wages if your identity is stolen.

You must sign up to take advantage of this free personal security protection. If you would like to take advantage of this free service, please contact us at [group email box]. We also recommend that you consider the following additional free services to protect you and your impacted beneficiaries.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322- 8228, or by 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf.

You also can contact one of the following three national credit reporting agencies:

- TransUnion P.O. Box 1000 Chester, PA 19016 1-800-909-8872 www.transunion.com
- Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com
- Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-685-1111 www.equifax.com

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud 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.

Security Freeze

Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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.

Additional Free Resources

You can obtain information from the consumer reporting agencies, the FTC or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state. You can find the contact information for your state's attorney general at https://www.usa.gov/state-attorney-general. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338.