CONDON TOBIN SLADEK THORNTON

Aaron Z. Tobin

Attorney at Law

214.265.3800
atobin@ctstlaw.com

Licensed in Texas and North Carolina

December 31, 2020

Via Email: DOJ-CPB@doj.nh.gov
Department of Justice
Attn: Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301

Re: NOTICE OF DATA BREACH PURSUANT TO STATE LAW

To the Office of the Attorney General:

This letter is sent on behalf of our client, Global Growth Holdings, Inc., to provide notice of a data breach pursuant to state law. Please contact us with any inquiries regarding this matter.

The Company

Global Growth Holdings, Inc., ("Global Growth"), is a Delaware corporation, located at 251 Little Falls Drive, Wilmington, Delaware, 19808. Its FEIN is 56-1996384, and its agent for service of process is Corporation Service Company at 251 Little Falls Drive, Wilmington, DE 19808.

Global Growth is the holding company for a portfolio of businesses operating in verticals including technology, communications, healthcare services, and financial services. Global Growth has over 100 employees and is not a HIPAA covered entity or a financial institution under GLBA.

Description of the Incident

On or around December 1, 2020, an unknown and unauthorized third-party gained access to the email account of an employee in the Global Growth Corporate Human Resources department. The company discovered the compromise on December 1, 2020 when Microsoft Office 365 alerted IT to suspicious behavior on the account. The company immediately took measures to terminate the unauthorized third-party's access.

Thereafter, the company changed the credentials of the employee whose account was accessed, took possession of her laptop, and re-imaged it to ensure there was no malware on the computer. The company also analyzed its logs to verify that the unauthorized third parties were no longer in the system. The company did not find any evidence that the unauthorized third party had access to its systems after the access was terminated on December 1.

Between December 1 and December 18, 2020, the company's internal and external incident response teams analyzed forensic evidence left by the unauthorized third-party to understand the impact of the attack. As a part of these efforts, which are ongoing, the business found evidence that the unauthorized third-party may have downloaded employee personal information as well as the personal information of former employees and employees' dependents ("impacted individuals") from the in-box of the HR employee.

From December 17 through the present (including over the Christmas holiday), the response team used artificial intelligence software to review the contents of the compromised e-mail account and identify potentially impacted individuals along with the personal information belonging to such impacted individuals for purposes of notifying them of the breach and taking steps to mitigate any harm to them.

The investigation is ongoing, and the company continues to monitor its networks for suspicious activity.

Personal Information Involved

This incident involved the personal information of some current and former employees of Global Growth and some of its affiliated companies 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

Steps Taken to Remediate the Breach

As discussed above, the business discovered the compromise on December 1, 2020 and immediately took measures to terminate the hacker's access, eliminate the possibility of malware or spyware in the environment, and to determine what harm may have occurred.

The business continues to monitor system logs for alerts and unusual activity in its e-mail system, and it is improving its internal security protocols to detect and avoid similar attacks in the future. For example, the business is implementing multi-factor authentication to increase the security of its password-protected systems.

Also, following the conclusion of the investigation of the event, the business will update policies and procedures, as needed, to prevent or mitigate similar future events.

In order to mitigate the effects on individuals whose data may have been compromised, Global Growth has or is doing the following :

- Notifying the impacted individuals beginning January 1, 2021 (sample notice encl.)
- Providing the impacted individuals with free identity theft protection services as described below

Identity Theft Prevention Services

Global Growth is committed to ensuring the protection of its current and former employees and their families. Therefore, Global Growth 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. 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.

Also enclosed is a description of the number of impacted individuals for this state. Please reach out to us if you have any questions or need additional information.

Very truly yours,

Aaron Z. Tobin

AZT/jls
Enclosures

DISCLOSURE OF NEW HAMPSHIRE INDIVIDUALS
IMPACTED BY GLOBAL GROWTH HOLDINGS, INC. DATA BREACH

One New Hampshire resident is being notified that their information was involved in the security breach.

NOTICE TO IMPACTED EMPLOYEES

Dear [Insert name]:

We have reason to believe that you and/or individuals named as beneficiaries under your employee benefit plans may have been impacted by the IT Security incident described in the enclosed "NOTICE OF EMPLOYEE DATA BREACH". Specifically, we believe the hacker(s) had access to and may have downloaded sensitive personal information about you and/or your beneficiaries. Please review the NOTICE OF EMPLOYEE DATA BREACH carefully for details about the nature of the attack and the steps we are taking to prevent such attacks in the future.

If, after reviewing both the NOTICE OF EMPLOYEE DATA BREACH and this notice, you have any questions, reach out to [include contact person and email/ telephone].

Identity Theft Prevention Services

We recognize that Global Growth's employees are its greatest asset, and Global Growth is committed to ensuring the protection of its 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 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 [email for group 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.