GT GreenbergTraurig

July 7, 2023

**VIA EMAIL**
Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Formella:

We represent Gates Corporation ("Gates) located at 1144 15th St, Suite 1400, Denver, CO 80202, and are writing to notify your office of an incident that may affect the security of some personal information relating to 68 New Hampshire residents.

Gates Corporation ("Gates") was the target of a ransomware attack on February 11, 2023. Gates believes it is likely that the attacker only wanted money and not the information on its computers but, in an abundance of caution, it is letting individuals know that their information may have been accessed by the attackers. Gates immediately notified law enforcement and engaged computer forensic experts who worked around the clock with their IT team to restore its systems from back-ups. The computer forensics experts have also confirmed that Gates' IT environment is free from this malicious software going forward. Because of Gates' planning and investments in updating and improving its IT infrastructure, Gates was able to restore and restart its production capabilities quickly and without having to pay the attackers. To be clear, Gates restoration was due to the tireless efforts of its global IT personnel, and it did not pay ransom to "decrypt" its servers and restore its operational capabilities. On May 15, 2023, Gates discovered that data containing personal information may had been exfiltrated from its IT environment.

Gates' investigation revealed that the encrypted server contained employee HR records which may have included

.

Gates had robust security safeguards in place at the time to prevent unauthorized remote access and extensive employee training on external threats however, this incident arose as the result of some employees responding to spoofing emails, granting access to the intruder. It should be noted that due to Gates' superior security and response protocols in place, what could be considered a devasting ransomware attack, shutting down the company's global operations, was resolved quickly with full operations restored within a matter of weeks. The detailed investigation into what happened, identify the affected information, and prepare notice, took longer.

Additionally, Gates is offering employees identity protection (credit monitoring and identity theft) services from Kroll.

On or about June 30, 2023, Gates began mailing notifications to all potentially affected individuals. An example of the notification is attached. Notification has also been made to the three major credit reporting agencies.

Should you have any questions regarding this notification or other aspects of the data security event, please contact me for any additional information.

Best regards,

Kevin M. Scott
Shareholder

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a data security incident that may have impacted some of your personal information, as required by applicable law. We take the security of your information very seriously, and we sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to help protect your information.

**What happened?**

As you are aware, we were the target of a ransomware attack on February 11, 2023. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that your information may have been accessed by the attackers.

We immediately notified law enforcement and engaged computer forensic experts who worked around the clock with our superb IT team to restore our systems from back-ups. The computer forensics experts have also confirmed that our IT environment is free from this malicious software going forward. Because of our planning and investments in updating and improving our IT infrastructure, we were able to restore and restart our production capabilities quickly and without having to pay the attackers. To be clear, our restoration was due to the tireless efforts of our global IT personnel, led by Diego Silva and his leadership team, and we did not pay ransom to "decrypt" our servers and restore our operational capabilities.

**What information was involved?**

On April 30, 2023, we discovered that data containing personal information was exfiltrated from our IT environment. While we have no reports of misuse of anyone's information, our investigation revealed that the encrypted servers contained your

**What we are doing.**

We take the security of your information seriously and have taken measures to reduce the likelihood of a future cyber-attack, including increasing threat detection and further restricting remote access to meet the continually evolving cyber threat.

In an abundance of caution, we are offering the services of Kroll to provide identity monitoring at no cost to you for

have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. These services are more extensive than the services we have offered to our employees through Allstate as part of our health/welfare programs, and we would encourage you to take advantage of these Kroll services as well.

Visit to activate and take advantage of your identity monitoring services.
*You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

**What you can do.**

Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and activate the identity monitoring services we are providing at no cost to you. We also recommend that you review the "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

**For more information.**

If you have any questions, please call , Monday through Friday from 8:00 am - 5:30 pm Central Time, excluding major U.S. holidays. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

KROLL

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### $1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ***IMPORTANT ADDITIONAL INFORMATION***

**For residents of *Iowa*:** *Y*ou are advised to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of *Oregon*:** *Y*ou are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of *New Mexico*:** You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

**For residents of *District of Columbia, Maryland, New York, North Carolina, and Rhode Island*:** You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**DC Attorney General**
400 6th Street NW
Washington, DC 20001
1-202-727-3400
www.oag.dc.gov

**Maryland Office of Attorney General**
200 St. Paul Pl
Baltimore, MD 21202
1-888-743-0023
https://www.marylandattorneygeneral.gov/

**New York Attorney General**
120 Broadway, 3rd Fl
New York, NY 10271
1-800-771-7755
www.ag.ny.gov

**North Carolina Attorney General**
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

**Rhode Island Attorney General**
150 South Main St
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

**Federal Trade Commission,** Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

***Massachusetts and Rhode Island residents*:** You have the right to obtain a police report if you are a victim of identity theft.

**For residents of all states:**

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

**Security Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

**Equifax Security Freeze**
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

**Experian Security Freeze**
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

**TransUnion Security Freeze**
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800