Baker & McKenzie LLP

815 Connecticut Avenue, N.W.
Washington, DC 20006-4078
United States

Tel: +1 202 452 7000
Fax: +1 202 452 7074
www.bakermckenzie.com

June 22, 2021

Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302

Re: Security Incident Report Pursuant to N.H. Rev. Stat. § 359-C:19

Dear New Hampshire Attorney General,

We are writing on behalf of Roto-Die Company, Inc., d/b/a RotoMetrics (collectively, "RotoMetrics") ("Company"), which was the victim of a cyber-incident that the investigation to date indicates occurred from May 7, 2021 to May 9, 2021. Our safeguards successfully stopped the threat actor before they could launch a ransomware attack to extort a payment from the Company. In response to this, we initiated an investigation to determine the scope of the incident and to confirm the restoration of the security and integrity of the systems. We engaged a leading third-party cybersecurity forensics firm to assist with the investigation. In the course of the investigation, our forensics firm determined that the threat actor was able to access and potentially exfiltrate some electronic folders before the Company was able to stop their access.

We are taking steps to protect the affected individuals in the event that any of the sensitive personal information was obtained by the threat actor. We have now confirmed that personal information relating to approximately 1,961 of our current or former employees was included in the accessed files, approximately forty-seven of which are New Hampshire residents.

We are providing notice to affected current and former employees. Notice to residents of New Hampshire will be sent on or about Wednesday, June 23, 2021. A copy of this notice is also enclosed. Impacted individuals are also being provided 24 months of credit monitoring services.

Current or former employees affected by this intrusion may contact their local HR partner or Brooke McClung, Global HR Director/Corporate Business Partner, either via e-mail at BMcClung@maxcessintl.com or by phone at 636-587-1120.

Please feel free to contact me with any questions at Michael.Egan@bakermckenzie.com or (202)-452-7022.

Best regards,

Michael C. Egan

June 23, 2021

[redacted]

NOTICE OF DATA BREACH

Dear [redacted]

We recently learned of a data security incident involving sensitive personal information of certain current and former employees of Roto-Die Company, Inc., d/b/a RotoMetrics ("RotoMetrics") as well as certain current employees of Maxcess Americas, Inc. ("Maxcess"). This incident included elements of your personal information. We take the protection of your information seriously. We are contacting you now to explain what happened and the steps you can take to protect yourself against possible identity fraud.

WHAT HAPPENED

RotoMetrics was the victim of a cyber-incident that the investigation to date indicates occurred from May 7, 2021 to May 9, 2021. Our safeguards successfully stopped the threat actor before they could launch a ransomware attack to extort a payment from the company. In response to this, we initiated an investigation to determine the scope of the incident and to confirm the restoration of the security and integrity of the systems. We engaged a leading third-party cybersecurity forensics firm to assist with the investigation. In the course of the investigation, our forensics firm determined that the threat actor was able to access and potentially exfiltrate some electronic folders before we were able to stop their access. We are taking steps to protect you in the event that any of your sensitive personal information in those folders was obtained by the threat actor.

WHAT INFORMATION WAS INVOLVED

In the course of our investigation, it was determined that employee records of certain current and former employees of RotoMetrics as well as certain current employees of Maxcess, which were stored on the RotoMetrics systems, were subject to unauthorized access. As a result, some of your sensitive personal information may have been included in folders that were accessed and potentially exfiltrated by the threat actor, specifically your social security number, your first and last name, date of birth, and postal address. At this point, we have no evidence that this information has been used to commit identity fraud or otherwise misused.

WHAT WE ARE DOING

In response to the findings from our investigation, we immediately took steps to protect our current and former employees. The safeguards we had already implemented prevented a ransomware attack from being launched. We also worked diligently to scan and review our systems to verify that they were safe to use after the attack. We continue to work closely with our external industry-leading partners to implement enhanced security measures to protect our systems, and to do what we can to help prevent this type of incident in the future.

WHAT YOU CAN DO

As mentioned above, at this point, we have no evidence that your sensitive personal information has been used to commit identity fraud or otherwise misused. Nonetheless, we encourage you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. If you are asked for personal or sensitive information from someone claiming to be from RotoMetrics, or Maxcess, verify the

authenticity of the request with company personnel. We encourages you to remain vigilant, review your account statements, and monitor your credit reports where available.

To help relieve concerns and restore confidence following this incident, we are offering you a two-year membership of Experian's® IdentityWorks^{SM}. 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**: September 30, 2021 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

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 **1-877-890-9332**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring**: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers. 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **1-877-890-9332**. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

OTHER IMPORTANT INFORMATION

Please consider the following additional information:

- You may wish to visit the website of the U.S. Federal Trade Commission at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
    - If you are a resident of North Carolina, you can reach your State Attorney General at (919) 716-6400 or at the following address: 9001 Mail Service Center, Raleigh, NC 27699-9001.

- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: *(1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint*. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
    - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
    - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
    - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000
- You have relevant rights pursuant to the federal Fair Credit Reporting Act. For more information, please see the U.S. Federal Trade Commission's bulletin on Fair Credit Reporting Act rights available here: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

FOR MORE INFORMATION

If you have further questions or concerns, please contact your local HR partner or Brooke McClung, Global HR Director/Corporate Business Partner, at BMcClung@maxcessintl.com or 636-587-1120.

Sincerely,

Roto-Die Company, Inc., d/b/a RotoMetrics