Withers Bergman LLP

430 Park Avenue, 10th Floor, New York, New York 10022-3505
t: +1 212 848 9800
f: +1 212 848 9888
www.withersworldwide.com

July 8, 2024

Attorney General Anthony Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
Email: idtheft@oag.state.md.us

VIA EMAIL

Re: Notice of Data Security Incident

To Whom It May Concern:

This firm represents BlueTriton Brands, Inc. ("BTB"), an American beverage company based in Stamford, Connecticut, in connection with a data security incident described in greater detail below. BTB understands the importance of protecting the personal information entrusted to it and is making this notification to your office in accordance with applicable law.

Beginning on or about June 11, 2024, persistent and unauthorized login attempts were detected on the Readyfresh® e-commerce platform. BTB's security and application support teams took prompt action to mitigate and contain the impact and to prevent further unauthorized access. BTB's investigation revealed that the incident was caused by "credential stuffing," a type of cyberattack where attackers use automated tools to attempt multiple login requests with stolen or leaked usernames or passwords. This attack exploits the common practice of individuals reusing their passwords across multiple sites, allowing attackers to gain unauthorized access to user accounts if the credentials match.

In this instance, username and password combinations were taken from another site and reused to gain access to certain ReadyRefresh® accounts. As a result of the investigation, it was determined that, once logged in, the attacker might have gained access to the name, address, email address, order history and last four numbers of the credit card on file for the applicable accounts. As a result, that data may have been exposed to the attackers, and some of the information may have been altered in certain accounts.

Accounts identified as affected by the incident have been temporarily disabled, and the passwords for all impacted accounts must be reset by the users. BTB has implemented and is continuing to implement new security protocols to enhance monitoring and manual IP address blocking to mitigate further threats, and has also implemented targeted web application firewall protections. BTB has notified law enforcement and continues to investigate the incident. BTB is also continuing to identify and implement measures to further strengthen its system security to help prevent similar attacks in the future.

As a result, on July 8, 2024, BTB is providing this notification of the incident via email in accordance with applicable law, including to twenty-three (23) Maryland residents. A sample copy of the notification letter is attached.

direct: +1 212 848 9855
fax: +1 212 824 4255
e-mail: doron.goldstein@withersworldwide.com

Should you have any questions or require additional information, please do not hesitate to contact the undersigned.

Very truly yours,

Doron S. Goldstein

Enclosures

[Date]

Account Number: [Acc]

NOTICE OF DATA BREACH

Dear [First_Name] [Last_Name],

We are writing on behalf of BlueTriton Brands, Inc. (“BTB”), to inform you of an incident that may have involved some of your personal data held by BTB. We take the protection of your personal data seriously and want to inform you about this incident, what we have done to remediate it, and steps you can take to protect yourself.

What Happened?
Beginning on or about June 11, 2024, persistent and unauthorized login attempts were detected on the Readyfresh® e-commerce platform. Our security and application support teams took prompt action to mitigate and contain the impact and prevent further unauthorized access.

What Information Was Involved?
Our investigation revealed that the incident was caused by “credential stuffing,” a type of cyberattack where attackers use automated tools to attempt multiple login requests with stolen or leaked usernames or passwords. This attack exploits the common practice of individuals reusing their passwords across multiple sites, allowing attackers to gain unauthorized access to user accounts if the credentials match.

In this instance, your username and password combination were taken from another site and reused to gain access to your ReadyRefresh® account. Once logged in, the attacker might have gained access to your name, address, email address, order history and last four numbers of your credit card on file. As a result, that data may have been exposed to the attackers, and some of your information may have been changed in your ReadyRefresh® account.

What We Are Doing.
Accounts identified as affected by the incident have been temporarily disabled, and the passwords for all impacted accounts must be reset by the users. We are implementing new security protocols to enhance monitoring and manual IP address blocking to mitigate further threats. We also implemented targeted web application firewall protections. We have notified law enforcement and continue to investigate this matter.

What You Can Do.

This incident was caused by the attacker having obtained access to your username and password from another account and using it to access your ReadyRefresh® account. That username/password combination can also be targeted by the attacker to any other site where you reused it. To protect yourself, you will need to change the passwords on every account where you reuse the same username/password combination and use a unique password for each of your online accounts.

Please also see the attached "Additional Actions To Help Reduce Your Chances of Identity Theft" which is part of this notice, for further general information on actions you can take to protect against identity theft.

For More Information.
We have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

If you have further questions or concerns about this incident, you can contact us at 1-800-274-5282 between 8:00 am and 6:00 pm Monday-Friday. We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,
ReadyRefresh® Customer Experience Team

* * * * * * * * *

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

> ORDER YOUR FREE ANNUAL CREDIT REPORTS

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide consumer reporting agencies. To order your annual free credit report, please visit www.annualcreditreport.com or call 1-877-322-8228. Contact information for the three nationwide consumer reporting agencies is as follows:

- **Equifax, PO Box 105281, Atlanta, GA 30348-5281. www.equifax.com, 1-888-378-4329**
- **Experian, PO Box 4500, Allen, TX 75013. www.experian.com, 1-888-397-3742**
- **TransUnion, PO Box 1000, Chester, PA 19016. www.transunion.com, 1-800-916-8800**

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the consumer reporting agency.

> USE TOOLS FROM CREDIT PROVIDERS

We recommend you remain vigilant for instances of fraud and identity theft. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a consumer reporting agency.

> PLACE A FRAUD ALERT ON YOUR CREDIT FILE

There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An initial fraud alert stays on your credit report for one year, while an extended fraud alert stays on your credit report for seven years and may be placed on your credit report if you have already been a victim of identity theft and have the appropriate documentary proof.

A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud or identity theft. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You can place a fraud alert on your credit report by contacting any one of the three nationwide consumer reporting agencies, who will contact the other two.

> **CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE**

You have a right to place a “security freeze” on your credit report, which is designed to prohibit the release of information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

Security freezes must be placed separately for each of the consumer reporting agencies. To place a security freeze on your credit report, you must send a separate request to each of the

three nationwide consumer reporting agencies online, by telephone, or by regular, certified, or overnight mail as provided below:

- **Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348-5788 1-888-298-0045**
  https://www.equifax.com/personal/credit-report-services/
- **Experian Security Freeze P.O. Box 9554, Allen, TX 75013 1-888-397-3742**
  https://www.experian.com/freeze/center.html
- **TransUnion Security Freeze, P.O. Box 160, Woodlyn, PA 19094 1-800-916-8800**
  https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The consumer reporting agencies have one business day if requested by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The consumer reporting agencies must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To temporarily lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must contact the consumer reporting agencies through their websites, via telephone, or by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The consumer reporting agencies have one hour if requested by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must contact each of the three consumer reporting agencies through their websites, by telephone (where permitted), or by mail and include proper identification (name, address, and social security number) and the PIN number or

password provided to you when you placed the security freeze. The consumer reporting agencies have one hour if requested by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

> REPORTING IDENTITY THEFT AND OBTAINING MORE INFORMATION ABOUT WAYS TO PROTECT YOURSELF

Federal Trade Commission and State Attorneys General. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should promptly contact the Federal Trade Commission and/or the Office of the Attorney General in your state. You can obtain information from these sources about steps you can take to identify and protect yourself against identity theft as well as information about fraud alerts and security freezes. The FTC may be reached at:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580. www.ftc.gov/idtheft, www.identitytheft.gov, ID Theft hotline: 1-877-IDTHEFT (438-4338).
- Police Reports. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should also contact your local law enforcement authorities and file a police report, and should consider obtaining a copy of the police report in case you are asked to provide copies to creditors to correct your records.

> RESIDENTS OF MARYLAND

Maryland residents can obtain information from the Maryland Attorney General about steps they can take to avoid identity theft at:
Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
1-888-743-0023 (toll-free in Maryland)
1-410-576-6491 (Identity Theft Unit direct line)
idtheft@oag.state.md.us
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

> RESIDENTS OF NEW YORK

New York residents may contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:
New York Department of State Division of Consumer Protection
One Commerce Plaza
99 Washington Ave.
Albany, NY 12231-0001
dos.ny.gov/consumerprotection

1-518-474-8583
1-800-697-1220

New York State Office of the Attorney General
The Capitol
Albany, NY 12224-0341
ag.ny.gov
1-800-771-7755

> RESIDENTS OF RHODE ISLAND

Under Rhode Island law, you have the right to file and obtain a copy of any police report filed regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Contact your local police department to file a report. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

Rhode Island law also allows consumers to place a security freeze on their credit reports. See above for details on security freezes, including how to place, temporarily lift, or permanently remove a security freeze on a credit report.

You can obtain information about steps you can take to help you prevent identity theft by contacting:
Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02983
riag.ri.gov
1-401-274-4400