Debevoise & Plimpton

Debevoise & Plimpton LLP
801 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
+1 202 383 8000

July 16, 2021

**BY ONLINE SUBMISSION**

Office of the Attorney General
109 Sewall St.
Augusta, ME 04330

To Whom It May Concern:

On behalf of The Food Group ("TFG"), this letter provides notice of a potential cybersecurity incident involving Maine residents. TFG is a for-profit advertising and marketing agency operating in the U.S. and its principal place of business is located at 3820 Northdale Blvd, Suite 202B, Tampa FL 33624. Based on currently known information, TFG believes approximately 2 potentially affected individuals reside in your jurisdiction.

On June 8, 2021, TFG discovered that it had experienced a ransomware incident in which several servers were encrypted by an unauthorized third party. On June 14, 2021, TFG first identified evidence indicating that the unauthorized third party had deployed tools which could have allowed it to exfiltrate data from TFG's environment, including personal information. The earliest known date of unauthorized third party activity in TFG's environment was on February 20, 2021. There has been no observed malicious activity in TFG's environment since June 7, 2021.

After becoming aware of the incident, TFG immediately took steps to prevent further unauthorized access. TFG promptly reported the incident to the Federal Bureau of Investigation and also began a thorough investigation with the support of outside cybersecurity experts. As noted above, on June 14, 2021, TFG first identified tools which could have potentially allowed the exfiltration of personal information.

TFG has not, however, confirmed any specific access or acquisition of personal information by the unauthorized third party. Nevertheless, out of an abundance of caution, TFG is notifying your office as well as individuals whose personal information was potentially accessible to the unauthorized third party.

The types of personal information that the unauthorized third party may have potentially acquired included current and former employee names and bank account details, stored for the purpose of writing checks. The system did not store individual Social Security Numbers or Tax IDs. TFG is also not aware of any

cases of identity theft, fraud, or financial losses to individuals stemming from this incident and does not believe the unauthorized third party was targeting personal information.

TFG anticipates sending all formal notices on or about July 21, 2021 via U.S. Mail. The notice to individuals was not delayed as a result of a law enforcement investigation.

A sample notification letter is enclosed. As stated in the attached sample notice, to protect individuals further, TFG is offering to provide 24 months of free identity theft and credit monitoring services through Equifax, notwithstanding that TFG has not confirmed actual access or exfiltration of their personal information.

Since discovering the incident, TFG is continuing to monitor and improve its capabilities to detect any further threats and prevent any further unauthorized activity. These steps include rebuilding affected servers, implementing mandatory multi-factor authentication, performing an enterprise–wide password reset, auditing administrator and service account privileges, and installing additional endpoint detection tools on workstations including Microsoft Defender.

TFG takes the protection of personal information seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at 1-202-430-9923 or ldembosky@debevoise.com.

Respectfully yours,

Luke Dembosky
Partner

Enclosure

the food group
CREATIVE FOOD+BEV MARKETING

July 21, 2021

[INSERT NAME]
[INSERT ADDRESS]

**NOTICE OF SECURITY INCIDENT**

Dear [FIRST NAME]:

We are writing to inform you of an incident potentially involving some of your personal information held by The Food Group ("TFG"). We want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

**WHAT HAPPENED?**

On June 8, 2021, we discovered that an unauthorized third party had gained remote access to our network in an effort to disrupt our operations. After becoming aware of the incident, we quickly took steps to secure our IT systems and have been investigating the incident with the support of outside cybersecurity experts. On June 14, 2021, we first identified evidence indicating that the unauthorized third party had deployed tools which could have allowed it to exfiltrate data from our environment, including personal information. We have not, however, confirmed any specific access or acquisition of personal information by the unauthorized third party. Nevertheless, we are notifying you out of an abundance of caution, to safeguard your interests.

**WHAT INFORMATION WAS INVOLVED?**

The types of personal information that the unauthorized third party could have acquired included your name and bank account details. However, TFG currently has no knowledge that your information has been misused, if it was acquired, and TFG does not believe the unauthorized third party was targeting personal information in the incident. The system did not store individual Social Security Numbers or Tax IDs.

July 21, 2021
Activation Code: _____
Expiration Date: October 31, 2021

**WHAT WE ARE DOING**

Upon discovering the incident, we quickly took steps to secure our systems. We have been investigating the incident to prevent recurrence with the help of leading outside cybersecurity experts and have introduced enhanced security controls. We have also notified law enforcement.

Although at this time we have no indication of any misuse of your information, as a precaution, we are offering a complimentary two-year membership of Equifax Credit Watch Gold (U.S.) which includes credit monitoring and identity theft protection services through Equifax.

Equifax® Credit Watch™ Gold provides you with the following key features:

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft

**Enrollment Instructions**

Go to **www.equifax.com/activate**
Enter your unique Activation Code of [X] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a My Equifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account**:
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**

Upon successful verification of your identity, you will see the Checkout Page.
Click 'Sign Me Up' to finish enrolling.

5. **You're done!**

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

You need to activate your membership in order to receive your benefits, and must do so no later than October 31, 2021. Your Activation Code will not work after this date.

If you have questions about our provision of this complementary credit monitoring service to you, please contact us at (866) 640-2273.

**WHAT YOU CAN DO**

We strongly encourage you to contact Equifax and take advantage of the credit monitoring and identify theft protection services we are offering to you free of charge. Remain vigilant and carefully review your financial accounts for any suspicious activity.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file where relevant.

**FOR MORE INFORMATION**

TFG sincerely regrets any inconvenience this incident has caused. If you have any questions, you can contact us at privacy@tfg.com.

***The Food Group***

July 21, 2021
Activation Code: _____
Expiration Date: October 31, 2021

## Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

**Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements 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 incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

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

**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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

| **Equifax**: | **Experian**: | **TransUnion**: |
|---|---|---|
| equifax.com<br>equifax.com/personal/credit-report-services<br>P.O. Box 740241<br>Atlanta, GA 30374<br>866-349-5191 | experian.com<br>experian.com/help<br>P.O. Box 2002<br>Allen, TX 75013<br>888-397-3742 | transunion.com<br>transunion.com/credit-help<br>P.O. Box 1000<br>Chester, PA 19016<br>888-909-8872 |

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security

number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

**Fraud Alert**

You may want to consider placing a fraud alert on your credit file. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

**Security Freeze**

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

**Federal Fair Credit Reporting Act Rights**

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**Additional Information**

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

**For Colorado, Delaware, and Illinois residents:** You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

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

**For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

**For Georgia, Maryland, New Jersey, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

**For New York residents:** You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

**For Rhode Island residents:** You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov/, (401) 274-4400.

**For Tennessee residents:**

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

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal

identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

(1) The personal identification number or password;

(2) Proper identification to verify your identity; and

(3) The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information. 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 fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.