

June 21, 2023

DELIVERED VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

Dear Sir or Madam:

On behalf of our client, Dole plc ("Dole"), we write to inform you of a cybersecurity incident that involved certain personal information associated with two (2) Maryland residents.

In February 2023, Dole was the victim of a sophisticated ransomware attack involving unauthorized access to employee information, which may have included information collected during the course of the employee's employment, such as name, address, date of birth, driver's license, Social Security number, and passport number. Upon detecting the attack, Dole promptly took steps to contain the attack, retained the services of leading third-party cybersecurity experts and notified law enforcement.

The incident was contained, and Dole has taken additional steps to help prevent future security incidents. To date, Dole has seen no evidence of misuse of the personal information of the Maryland residents impacted in the incident.

In an abundance of caution, however, Dole is offering a complimentary one-year membership to Equifax ID Watchdog to the impacted Maryland residents. Additionally, Dole is providing the impacted individuals with guidance on how to protect against identity theft, including information on placing a fraud alert or credit freeze on their credit files, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and contact information for the Federal Trade Commission and the three major credit bureaus.

A copy of a representative template that will be used to mail notices to the impacted Maryland residents is attached as **Exhibit A**.

Thank you for your attention to this matter.

Sincerely,

/s/ Stephenie Handler

Gibson, Dunn & Crutcher LLP

EXHIBIT A



June 20th, 2023

Sample Notice of Data Breach

Dear [Name]:

We are writing to inform you of a cybersecurity incident that may have involved certain personal information about you. We are contacting you to explain the circumstances of the incident, the types of information involved, what we are doing and have done in response to the breach, and steps that can be taken to help protect your information.

What happened? In February 2023, we became aware of a ransomware attack affecting certain of our systems containing employee personal data. We promptly launched an investigation, notified law enforcement, and engaged leading cybersecurity firms to assist in assessing the scope of and containing the incident, as well as to restore and resecure impacted data. We have no reason to believe that your personal data was or will be subject to any fraudulent misuse. Out of an abundance of caution, however, we are notifying all U.S. Fresh Fruit employees of the incident and providing complimentary 1-year credit monitoring.

What information was involved? The information varies by individual, but may include information collected in the course of your employment with us, such as your name, address, telephone number, driver's license, Social Security number, Passport numbers, date of birth, and/or other employment related information.

What we are doing. We are working with leading cybersecurity firms to support our investigation and are taking additional security steps to enhance our security and help prevent future incidents. We are continuing to monitor the dark web for any indication of misuse of personal information in connection with this incident, and to date have not identified any such misuse. As an added precaution to help protect your identity, we are also offering a complimentary 1-year membership of Equifax ID Watchdog. You will be sent instructions directly from Equifax shortly.

What can you do? While there is no indication of fraud resulting from this incident, in addition to enrolling in the identity theft protection services described below, we encourage you to remain vigilant with respect to your personal accounts. We would also encourage you, as always, to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information. Please also refer to the enclosure entitled "Information about Identity Theft Protection" for additional actions you should consider taking to protect yourself against fraud and identity theft.

We take the privacy and security of your information very seriously. We sincerely regret any concern or inconvenience this matter may cause you.

Sincerely,

Dole Food Company

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 303485281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-
0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9702
Allen, TX 75013-
9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-
1000
1-800-888-
4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-
9554
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-
2000
1-888-909-
8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/m/freeze/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at

www.privacy.ca.gov to find more information about your medical privacy.

Federal Trade Commission and State Attorneys General Offices

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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft, including the use of fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438- 4338). Residents of Maryland can obtain more information about preventing and avoiding identity theft from their Attorney General using the following information: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.