

ALSTON & BIRD

The Atlantic Building
950 F Street, NW
Washington, DC 20004-1404
202-239-3300 | Fax: 202-239-3333

Kimberly Peretti

Direct Dial: 202-239-3720

kimberly.peretti@alston.com

May 16, 2023

CONFIDENTIAL
VIA E-MAIL

Office of the Maryland Attorney General
IDTheft@oag.state.md.us

Re: Notice of Data Security Incident

To the Maryland Attorney General's Office:

We are writing on behalf of Fresh Del Monte Produce, Inc. ("Fresh Del Monte") to notify you of a data security incident. A copy of the notification being sent to two (2) Maryland residents on May 16, 2023 by first class mail in accordance with notification requirements under state law is attached to this letter.

On January 13, 2023, Fresh Del Monte discovered that certain systems within its network may have been subject to unauthorized activity. Upon discovery, Fresh Del Monte immediately launched a thorough investigation and took its systems offline to help contain the incident. As part of this process, a leading forensics firm was engaged to assist with investigation and remediation efforts. Through the investigation, Fresh Del Monte learned that an unauthorized third party accessed and removed some data from certain systems containing personal information of individuals on January 13, 2023. It then conducted a comprehensive review of the impacted data to determine what information was affected and to whom the information related. This review was completed on April 25, 2023.

The personal data involved in this incident may have included an individual's name in combination with one or more of the following elements: (1) health insurance information; and/or (2) username and password. Please note that not all data elements were involved for all individuals.

The security and integrity of its systems are a top priority for Fresh Del Monte. As soon as it discovered the incident, Fresh Del Monte immediately took action to stop the unauthorized activity. This included launching a forensic investigation and proactively taking all of its systems offline to help contain the incident. Fresh Del Monte also retained a third-party cybersecurity forensic firm to investigate the issue and reported the incident to U.S. law enforcement. In response to this incident, Fresh Del Monte has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future.

Free credit monitoring services for 12 months are being offered to all individuals whose personal information may have been involved.

Re: Notice of Data Security Incident
May 16, 2023
Page 2

If you have any questions regarding this incident or if you desire further information or assistance, please email me at kimberly.peretti@alston.com or call my direct line at 202-239-3720.

Sincerely,

A handwritten signature in dark ink, appearing to read "K Peretti". The signature is written in a cursive, slightly stylized font.

Kimberly Peretti

Enclosure



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

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

Notice of Data Breach

To <<First_Name>> <<Last_Name>>,

We are writing to inform you of a data security incident that occurred at Fresh Del Monte Produce, Inc. (“Fresh Del Monte,” “we,” or “our”) that may have affected your personal information. We are committed to protecting your information. This commitment includes notifying you if we believe that an incident may have involved your personal information. This letter provides information about the incident and the resources available to you.

What Happened?

On January 13, 2023, we discovered that certain systems within our network may have been subject to unauthorized activity. Upon discovery, we immediately launched a thorough investigation and took our systems offline to help contain the incident. As part of this process, a leading forensics firm was engaged to assist with investigation and remediation efforts. Through our investigation, we learned that an unauthorized third party accessed and removed some data from certain systems containing personal information of individuals on January 13, 2023. Based on data analysis which was completed on April 25, 2023, we learned that your personal information may have been involved.

What Information May Have Been Involved?

Based on the review, the personal information involved in this incident may have included your name in combination with one or more of the following elements: (1) Social Security number; (2) driver’s license number, passport number, or other government-issued ID; (3) financial account information; (4) medical and/or treatment information; (5) health insurance information; and/or (6) username and password. Please note that not all data elements were involved for all individuals.

What We Are Doing.

The security and integrity of our systems are a top priority for Fresh Del Monte. As soon as we discovered the incident, we immediately took action to stop the unauthorized activity. This included launching a forensic investigation and proactively taking all of our systems offline to help contain the incident. We also retained a third-party cybersecurity forensic firm to investigate the issue and reported the incident to law enforcement. In response to this incident, Fresh Del Monte has enhanced its security and monitoring as well as further hardened its systems as appropriate to minimize the risk of any similar incident in the future.

We have also arranged to offer you identity monitoring services for a period of 12 months, at no cost to you, through Kroll. You have until <<b2b_text_6(ActivationDeadline)>> to activate these services. Instructions on how to activate these services are included in the attached Reference Guide.

What You Can Do.

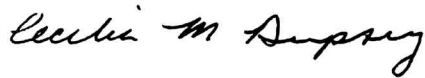
In addition to activating your complimentary identity monitoring services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and help protect your personal information. We also encourage you to carefully review all credit reports and statements sent from financial institutions to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company where you maintain the account.

For More Information:

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide or call toll-free (866) 347-2759. This call center is open from 9 am – 6:30 pm Eastern Time, Monday through Friday, excluding some major U.S. holidays.

We sincerely regret any inconvenience this incident may cause you and want to assure you that we take this matter seriously.

Sincerely,



Cecelia Dempsey
Chief Global Privacy Officer

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from your financial institutions to ensure that all your account activity is valid. Report any questionable charges promptly to the company where you maintain the account.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form. Once the verification process is complete, your credit report should be mailed to you within 15 days.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible, so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Activate Your Identity Monitoring Services

As a safeguard, we have arranged for you to enroll, at no cost, in identity monitoring services provided by Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<MembershipNumber (S_N)>>

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



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 will 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.

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.

The monitoring included in the membership must be activated to be effective. You have until **<<b2b_text_6(ActivationDeadline)>>** to activate these services. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

If you need assistance, please call (866) 347-2759, 9 am – 6:30 pm Eastern Time, Monday through Friday, excluding some major U.S. holidays.

We encourage you to take advantage of these protection services and remain vigilant for incidents of fraud and identity theft, moving forward, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any identity theft or fraud incidents, promptly report the matter to your local law enforcement authorities, state Attorney General, and the FTC.

You can contact the FTC to learn more about how to help protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To help protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud

alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze on your credit, potential creditors and other third parties will not be able to access your credit report unless you lift the freeze. This means, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy is legible, displays your name and current mailing address, and the date of issue.

Below is the relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze on your account no later than one (1) business day after receiving a request by phone or secure electronic means, and no later than three (3) business days after receiving a request by mail. No later than five (5) business days after a security freeze is placed on your account, the credit reporting agency will send you confirmation and information on how you can remove the security freeze in the future.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>.