Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Alyssa R. Watzman, Partner, Vice Chair
Cybersecurity & Data Privacy Team
1801 Broadway, Suite 500
Denver, Colorado 80202
Awatzman@constangy.com
Direct: 720.536.3234

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

October 29, 2026

VIA ONLINE SUBMISSION

Attorney General Nick Brown
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Del Monte Foods Corporation II Inc. ("Del Monte").[1] We are writing to provide notice of a data security incident experienced by Del Monte in February 2026 (the "Incident"), in connection with which individuals whose personal information was involved were recently identified.

By providing this notice, Del Monte does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data security incident notification statute, personal jurisdiction, or any other potentially applicable right or defenses.

1. Nature of the Incident

On February 9, 2026, Del Monte learned that it had experienced an issue impacting network operability and immediately initiated an investigation of the matter. Del Monte engaged cybersecurity experts to assist with the process. As a result of the investigation, Del Monte learned that certain files were acquired without authorization. Del Monte engaged a vendor to undertake a comprehensive review of those files and, on or about August 20, 2026, discovered that certain personal information was contained therein. Del Monte then worked diligently to obtain and verify address information sufficient to provide notice to individuals involved. This important step required additional time to complete given the need to coordinate with Fresh Del Monte in light of the sale of substantially all Del Monte assets and operations thereto. Address identification efforts concluded on October 20, 2026, after which Del Monte worked promptly to provide notice.

The potentially involved information includes first and last name as well as Social Security number, driver's license or government issued ID number, passport number, and medical or insurance information.

[1] Please note, as later indicated herein, Del Monte Foods Corporation II, Inc. filed for Chapter 11 bankruptcy, and substantially all of its assets have been acquired by unaffiliated purchasers as of March 19, 2026.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

2. Notice to Washington Residents

On October 29, 2026, Del Monte provided written notice of this Incident to approximately 4,821 Washington residents. A sample copy of the notification letter is being provided with this correspondence.

3. Other Steps Taken and To Be Taken

Upon discovering this Incident, Del Monte moved quickly to investigate and respond, ensure the security of its network, and identify potentially involved data / individuals in order to provide notice. Del Monte also worked to implement additional safeguards to bolster its security. For all notified individuals, Del Monte is providing access to 12 months of identity protection services, through Kroll, at no cost to these individuals.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the Incident, please contact me at awatzman@constangy.com. Please include Seth Greenwald (sgreenwald@constangy.com) on any correspondence.

Very truly yours,



Alyssa Watzman of
Constangy, Brooks, Smith & Prophete LLP

Attachment: Sample Notification Letter

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

To Enroll, Please Call: (844) 971-8616
Or Visit: https://enroll.krollmonitoring.com
Enrollment Code: **<<Activation Code s_n>>**



<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

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

<<b2b_text_1 (Subject: Notice of Data Security Incident / Breach)>>

Dear <<First_name>> <<Last_name>>:

We are writing to inform you of a data security incident that may have involved your personal information. Del Monte Foods Corporation II Inc. ("Del Monte") takes the privacy and security of all information very seriously. This letter contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened. On February 9, 2026, Del Monte learned that it had experienced an issue impacting network operability and immediately initiated an investigation of the matter. Del Monte engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files were acquired without authorization. Del Monte undertook a comprehensive review of those files and, on or about August 20, 2026, learned that certain personal information was contained therein which is the reason for this notification. Thereafter, Del Monte worked to confirm addresses sufficient to effectuate notice, which was completed on October 20, 2026. Upon completion of that process, Del Monte then worked quickly to provide you with this notice.

What Information Was Involved. The potentially involved information includes your name as well as your <<b2b_text_2 (Affected Regulated Data Sets)>>.

What We Are Doing. As soon as Del Monte learned of this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. Del Monte will also cooperate with any law enforcement investigation of this incident to hold the perpetrator(s) accountable. Del Monte is also offering you complimentary identity protection services through Kroll, a leader in consumer identity protection. These services include <<ServiceTerminMonths>> months of credit monitoring[1], dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is <<b2b_text_6 (activation deadline)>>.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary services offered to you through Kroll by using the enrollment code provided above.

For More Information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call (844) 971-8616 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Del Monte Foods Corporation II Inc.

[1] To receive credit monitoring 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.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies, Equifax, Experian, and TransUnion by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. AnnualCreditReport.com allows you to request your credit reports from the three nationwide credit reporting agencies through one centralized website. Free weekly online access to your credit reports is currently available. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert, contact any of the three credit reporting agencies using the contact information provided below. Additional information is available at www.annualcreditreport.com.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/fraud-alert/	https://www.transunion.com/fraud-alerts

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit, loans, and services from being opened in your name without your consent. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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 insurance statement. To place a security freeze, contact any of the three credit reporting agencies using the contact information provided below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
888-298-0045	888-397-3742	833-799-5355
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/credit-freeze/	https://www.transunion.com/credit-freeze

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Thank you for using version 2025.4.1104.462 of Telerik Document Processing Libraries. Access to the latest updates and support requires a valid license. Renew your license and download a new license key. Learn more about Telerik Document Processing Libraries licensing https://prgress.co/3PwQMut

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
916-445-9555

New York Attorney General
The Capitol
Albany, NY 12224
ag.ny.gov
800-771-7755

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400
11 RI residents were notified of this incident.

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
https://ag.ny.gov/resources/individuals/consumer-issues/technology
212-416-8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers
877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

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'll 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. 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.

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.