Kim Detwiler, Partner
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
kdetwiler@constangy.com
Mobile: 484.999.1307

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

October 23, 2026

VIA EMAIL
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301

Re: Notice of Data Event

To Whom It May Concern:

We represent A&L Foods, Inc. ("A&L"), located at 4200 Amos Avenue, Baltimore, MD 21215, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately one New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, A&L does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On July 3, 2026, A&L detected suspicious activity within its network. A&L promptly initiated an investigation of the matter and engaged cybersecurity specialists to assist with the incident response. As a result, A&L determined that certain files may have been accessed or acquired without authorization. A&L then conducted a comprehensive review of the affected data and learned that certain personal information was involved. A&L worked with a third-party vendor to obtain the relevant information that was necessary to effectuate formal notification. This process was completed on October 16, 2026.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to New Hampshire Residents

On or about October 23, 2026, A&L provided written notice of this incident to approximately one New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

3. Other Steps Taken and To Be Taken

Upon discovering the event, A&L moved quickly to investigate and respond to the incident, assess the security of its network, and identify potentially affected individuals. Further, A&L notified the Federal Bureau of Investigation regarding the event. A&L is providing access to credit monitoring services for twelve (12) months through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, A&L is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. A&L is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at 484.999.1307.

Very truly yours,



Kim Detwiler of
Constangy, Brooks, Smith & Prophete LLP

Exhibit A

A&L Foods, Inc.
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

[redacted]

October 23, 2026

Subject: Notice of Data Security Incident

Dear [redacted]:

We are writing to inform you of a data security incident that may have involved your personal information. A&L Foods, Inc. takes the privacy and security of the data under our care very seriously and we regret any concern or inconvenience this may cause. Please read this letter carefully as it contains information regarding the incident and steps you should take to help protect your personal information.

What Happened. On July 3, 2026, we detected suspicious activity within our network. We promptly initiated an investigation of the matter and engaged cybersecurity specialists to assist with the incident response. As a result, we determined that certain files may have been accessed or acquired without authorization. We then conducted a comprehensive review of the affected data and learned that certain personal information was involved. We worked with a third-party vendor to obtain the relevant information that was necessary to effectuate formal notification. This process was complete on October 16, 2026.

What Information Was Involved. The information may have included your name, as well as your Social Security number.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. Additionally, we have fully reviewed all of our internal networks and procedures. We have implemented new advanced measures to further enhance network security and minimize the risk of a similar incident occurring in the future. Some of these procedures like scheduled password changes will be obvious to you and many will not be as obvious. We are also providing access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or if you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

We strongly encourage you to participate in these credit monitoring services. To enroll in the Credit Monitoring services, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. There is no cost to you. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do. We recommend you read the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through TransUnion at no cost to you. 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.

You can enroll in the TransUnion identity protection services by calling 1-800-405-6108 or by going to https://bfs.cyberscout.com/activate and using the Enrollment Code provided above. You must enroll within 90 days from the date of this letter. TransUnion representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays.

For More Information. If you have questions, please call TransUnion 1-800-405-6108, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time. TransUnion representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

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,

A&L Foods, Inc.
4200 Amos Avenue
Baltimore, MD 21215

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 once every 12 months 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. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-833-799-5355
www.transunion.com/get-credit-report

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 on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com. For TransUnion: 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. 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. For TransUnion: 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.

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/Pages/CPD
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
800-952-5225

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

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

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
www.dos.ny.gov/
consumerprotection/
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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.