One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

MINTZ

April 7, 2023

VIA EMAIL – DOJ-CPB@doj.nh.gov

The Honorable John Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Reporting of Security Incident Pursuant to N.H. Rev. Stat. § 359-C:21 – CORRECTED NOTICE

Dear Attorney General Formella:

We are writing on behalf of Baldor Specialty Foods ("Company") to advise you of an incident that may affect the security of personal information relating to approximately 4 New Hampshire residents.

The Company was alerted on February 25, 2023 that a malicious actor had exploited a vulnerability and disabled the Company's security products to gain access to certain Company systems as well as various network resources and files. Upon learning of the incident, the Company immediately took steps to isolate and secure its systems and investigate the incident. The Company retained a nationally-known third-party forensics firm to determine the nature and scope of the intrusion. Through the Company's continued investigation, the Company became aware that, between February 7 and February 25, 2023, the attacker accessed and exfiltrated files containing personal information, and since then, has worked diligently to identify which files and which individuals may have been affected. As a result of the Company's internal investigation, it was determined that the files accessed and exfiltrated by the attacker contained personal information including

There is no indication that the personal information was retained or shared.

The Company is taking this incident very seriously, and has taken a number of steps to strengthen the protection of personal information and mitigate risk to protect from further types of attacks, including resetting all user credentials and extending its implementation of multi-factor authentication. In addition, the Company has rebuilt certain systems and is retiring others and has implemented endpoint detection software. The Company continues to closely monitor its network and information systems for unusual activity. The Company will also continue to further improve security across the Company networks and protect from unauthorized access or similar criminal activity in the future.

The Company is not aware of any fraudulent or malicious use of personal information of the affected New Hampshire residents at this time. The Company is sending the attached notices to affected New Hampshire residents on April 7, 2023, and the Company has arranged to make credit monitoring and identity protection services by IDX available to them at no cost for two (2) years. This includes access to assist individuals with credit restoration, a $1,000,000 insurance reimbursement policy, and credit monitoring services as described in the attached form of notice.

Please contact the undersigned at should you need further information or have any additional questions. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Sincerely,

Cynthia J. Larose

Attachment

ENROLL IN IDENTITY THEFT PROTECTION SERVICES

Call: 1-833-753-4651
OR
Visit: https://app.idx.us/account-creation/protect

Refer to enrollment code: <<Enrollment Code>>

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

April 7, 2023

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of an incident that may have affected your personal information.

On February 25, 2023, Baldor Specialty Foods received an initial indication that we sustained a cyberattack. We immediately took steps to isolate and secure our systems and investigate the incident. In addition, we immediately retained a leading cybersecurity firm to conduct a thorough investigation of the incident, remediate any risks, and methodically bring our systems back online.

The investigation revealed that the malicious actor accessed certain Baldor systems at various times from February 7, 2023 to February 25, 2023. During this time period, the malicious actor acquired certain files from our systems, including documents that may have contained some of your personal information. However, Baldor was able to quickly recover and there is no indication that the data was retained or shared. Therefore, we have no reason to suspect your information will be used for malicious purposes.

What Information Was Involved?

The type of information that was potentially compromised included information that we collected for human resources purposes, such as .
You may be receiving this letter as the spouse or dependent of an employee or former employee of Baldor.

What is Baldor Doing?

We have added advanced cybersecurity detection and monitoring tools on our newly restored systems for an additional layer of security and visibility across our network. We will also continue to make infrastructure enhancements to continuously strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

We are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To receive credit services, you must be over the age of 18, 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. If you do not have a credit file, you will not be able to register for credit monitoring services, but you will receive CyberScan monitoring, insurance, and the fully managed identity recovery services from IDX.

What Can You Do?

Although we have no evidence that your personal information will be used for fraudulent purposes, you should always remain vigilant and review statements and credit reports. Refer to the attached "Recommended Steps" for further information.

At this time, we have not received any reports that personal information has been subject to fraudulent activity. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-753-4651 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 7, 2023.

Please call 1-833-753-4651 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Michael Muzyk,
President
(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-753-4651 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to your within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Masssachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See Section 6 above for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400 There were 9 Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.