



Durango Coca-Cola
75 Girard Street,
Durango, CO 81303
970-247-1560

August 11, 2023

Via E-Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

I write on behalf of Durango Coca-Cola (the “Company”) to provide notice of a security incident potentially affecting one Maryland resident.

On May 22, 2023, an unauthorized third party attempted to gain access to the Company’s network and was able to encrypt data on the Company’s servers as part of a ransomware attack. Upon discovering the incident, the Company’s IT team immediately worked to secure its servers. Instead of giving into a ransomware demand from an unauthorized third party, we worked as quickly as possible—with the assistance of a leading third-party cybersecurity firm—to restore the Company’s systems and secure the Company’s network against any future attack. At the same time, the cybersecurity firm performed a comprehensive investigation into the incident to determine the scope of information that may have been accessed by the unauthorized third party. Ultimately, this investigation could not rule out the possibility that the unauthorized third party may have accessed documents containing individuals’ personal information that are stored on the Company’s network.

Upon identifying these documents, the Company retained the cybersecurity firm to review them for personal information and affected individuals. The Company received the initial list of potentially affected individuals on July 13, 2023. Consequently, the Company discovered that the documents identified contained the personal information of one Maryland resident, including their name and Social Security number.

The Company has sent the attached notification to the potentially affected Maryland resident. Out of an abundance of caution, we also offered one year of identity theft protection services at no cost to potentially affected individuals.

The Company has also contacted law enforcement regarding this incident and will cooperate in their investigations.

If you have any questions concerning this matter, please do not hesitate to contact our counsel Mr. Kwabena Appenteng at Kappenteng@littler.com, and Mr. Andrew Gray at Argray@littler.com.



Durango Coca-Cola
75 Girard Street,
Durango, CO 81303
970-247-1560

Very truly yours,

Meredith Mapel
President & CEO
Durango Coca Cola



Return mail will be processed by: IBC
PO Box 847
Holbrook, NY 11741

[NAME]
[MAILING ADDRESS]
[CITY], [STATE] [ZIP CODE]

August 11, 2023

Dear [NAME]:

Durango Coca-Cola (the "Company") values its employees, both current and former, and is committed to protecting your personal information. Unfortunately, I am writing to inform you of a security incident recently suffered by our Company. We currently have no reason to believe that your personal information has been misused as a result of this incident. The purpose of this letter is to apprise you of what transpired and the steps the Company has taken in the wake of the security incident.

On May 22, 2023, an unauthorized third party attempted to gain access to the Company's network and was able to encrypt data on our servers as part of a ransomware attack. Upon discovering the incident, the Company's IT team immediately worked to secure its servers. Instead of giving into a ransomware demand from an unauthorized third party, we worked as quickly as possible—with the assistance of a leading third-party cybersecurity firm—to restore the Company's systems and secure our network against any future attack. At the same time, the cybersecurity firm performed a comprehensive investigation into the incident to determine the scope of information that may have been accessed by the unauthorized third party. Ultimately, this investigation could not rule out the possibility that the unauthorized third party may have accessed documents containing your personal information that are stored on our network.

The potentially compromised documents include the following categories of your personal information: name, and Social Security number. **Please note that we have no information indicating that your personal information has actually been taken or otherwise misused.** Also, the documents in question did not contain any of your other sensitive information, such as your credit or debit card information or other financial account information.

Out of an abundance of caution, the Company is offering you one year of identity protection services, at no cost to you, through Experian, one of the three nationwide credit bureaus. Your one-year membership in Experian's IdentityWorksSM product provides identity restoration services, fraud detection tools, dark web monitoring, and other benefits, which include monitoring your credit file at Experian.

Starting today, you can call Experian's identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until September 30, 2023, by calling Experian at 1-877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate the fraud detection tools available through IdentityWorks. This product provides you with identity detection, credit monitoring, and resolution of identity theft.

If you wish to enroll in IdentityWorks, you will need to do the following:

1. **Visit** the IdentityWorks web site: <https://www.experianidworks.com/plus> or call 1-877-890-9332 to enroll and provide Engagement Number **[NUMBER]**.
2. **PROVIDE** your Activation Code: **[CODE]**

Enrollment Deadline: **September 30, 2023** (your Activation Code will not work after this date).

If you have any questions concerning IdentityWorks, or if you prefer to enroll over the phone for delivery of your membership via U.S. mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number **[NUMBER]** as proof of eligibility for the identity protection product by Experian.

In addition to the offer of IdentityWorks, included with this letter is additional information on steps you can take to protect the security of your personal information. I urge you to review this information carefully.

Please be assured that the Company takes seriously both the security of your personal information and this incident. In addition to the immediate actions described above, the Company is taking the necessary steps to ensure that this does not happen again. We have also reported this incident to law enforcement, and we will cooperate in any investigation.

The Company regrets this incident and any inconvenience it may cause you. Should you have any questions or concerns regarding this incident, please do not hesitate to contact the call center we have established at **[NUMBER]** between 8 A.M. and 6 P.M (CST), Monday through Friday.

Sincerely,

A handwritten signature in cursive script, appearing to read 'Meredith Mapel', written in dark ink.

Meredith Mapel
President & CEO
Durango Coca-Cola

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorks. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorks membership. Experian's IdentityWorks product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only¹.
- **Credit Monitoring:** Actively monitors your credit files at Experian for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Dark Web Surveillance:** Daily scans of over 600,000 web pages to detect if your information is stolen.
- **Experian IdentityWorks ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorks membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorks product to Experian. A credit card is not required for enrollment in IdentityWorks. Enrollment in IdentityWorks will not affect your credit score. The Terms and Conditions for this offer are located at: www.ExperianIDWorks.com/restoration.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled to one free copy of your credit report from each of the three national credit bureaus every 12 months. Until December 31, 2023, however, you are entitled to a free copy of your credit report from each of the three national credit bureaus once a week. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. Errors in information in your credit report may be a sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your credit report, whether or not due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorks identity resolution agent toll-free at 1-877-890-9332 or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to the Company, your local police department, your state's attorney general, and the Federal Trade Commission.

5. You have the right to place a "security freeze" on your credit report. A security freeze will prohibit a consumer reporting agency from releasing information in your credit file without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please understand that placing a security freeze on your credit file may delay, interfere with, or prevent the timely approval of any subsequent request or application you make for a new loan, mortgage, or any other account involving the extension of credit.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

To place a security freeze on your credit file, contact the three nationwide credit bureaus, listed below. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. There is no charge to place a credit freeze.

The contact information for all three credit bureaus is as follows:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

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

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; <http://www.ftc.gov/idtheft/>; (877) IDTHEFT (438-4338).

If you live in Maryland, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

If you live in New Mexico, please read the additional notice below that applies to you:

Please visit the following link to review a summary of your major rights under the federal Fair Credit Reporting Act (FCRA):
https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf.