

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Weaver does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 7, 2022, Weaver identified suspicious activity related to certain systems within its environment. Weaver immediately took steps to secure its network, and launched an investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, Weaver determined that an unknown actor may have had access to certain systems on June 16, 2022, through July 7, 2022. As a result, certain files within these systems and information may have been accessed or acquired by the unauthorized actor during this incident. Weaver quickly began a diligent and comprehensive review to identify information that may have been contained within the impacted files and to identify the individuals whose information may have been present. On January 3, 2023, Weaver concluded this review and determined that certain information related to certain individuals may have been accessed or acquired without authorization.

The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to Maine Residents

On or about February 1, 2023, Weaver began providing written notice of this incident to two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Weaver moved quickly to investigate and respond to the incident, assess the security of Weaver systems, and identify potentially affected individuals. Further, Weaver notified federal law enforcement regarding the event. Weaver is also working to implement additional safeguards and training to its employees. Weaver is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Weaver is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Weaver is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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. Weaver also notified law enforcement of the incident and is cooperating with its investigation.

Weaver is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



**WEAVER POPCORN
MANUFACTURING**

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 1, 2023

i9647-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF [Extra1]

Dear Sample A. Sample:

Weaver Popcorn Manufacturing, Inc. (“Weaver”) writes to inform you of a recent incident that may impact the privacy of some of your information. While we are unaware of any attempted or actual misuse of your information at this time, we are providing you with this notice in an abundance of caution, to inform you of the incident, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On July 7, 2022, Weaver identified suspicious activity related to certain systems within our environment. We immediately took steps to secure our network, and launched an investigation, with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, we determined that an unknown actor may have had access to certain systems on June 16, 2022 through July 7, 2022. As a result, certain files within these systems and information may have been accessed or acquired by the unauthorized actor during this incident. We quickly began a diligent and comprehensive review to identify information that may have been contained within the impacted files and to identify the individuals whose information may have been present. We are notifying you because the investigation recently determined information related to you was contained within the files.

What Information Was Involved? The review determined the information that may have been impacted by this incident includes your name and [Extra3]. At this time, we have no evidence that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among Weaver’s highest priorities. Upon learning of the incident, we took immediate steps to secure our environment and investigate the activity. We commenced an investigation that included working with third-party forensic specialists to understand the nature and scope of the incident. We also notified federal law enforcement about this incident and are cooperating with their investigation. While Weaver had policies and procedures regarding data security, as part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures, and processes related to the storage and access of sensitive information, and additional workforce training is being conducted to reduce the likelihood of a similar future incident. We are also notifying applicable regulatory authorities, as required by law.

0000001



As an added precaution, we are also offering 12 months of complimentary access to credit monitoring services through Experian. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to activate them on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at (833) 549-2138, toll-free Monday through Friday from 8 a.m. to 10 p.m. Central, or Saturday and Sunday from 10 a.m. to 7 p.m. Central (excluding major U.S. holidays). Please be prepared to provide Engagement Number B084505. You may also write to Weaver at 4485 South Perry Worth Road, Whitestown, IN 46075.

Sincerely,

Weaver Popcorn Manufacturing, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by April 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 549-2138** by April 30, 2023. Be prepared to provide engagement number **B084505** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

** 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected

identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For 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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Weaver is located at 4485 South Perry Worth Road, Whitestown, IN 46075.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting 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 Act, the consumer reporting bureaus 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 violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

