



Liberty Building, 420 Main Street, Suite 1110, Buffalo, New York 14202
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300 #704, Bala Cynwyd, Pennsylvania 19004
75 S. Clinton Ave, 510 Clinton Square, Suite 555, Rochester, New York 14604

December 8, 2021

VIA EMAIL

Office of the Idaho Attorney General
Consumer Protection Division
700 W. Jefferson Street
Boise, ID 83720-0010
agwasden@ag.idaho.gov

RECEIVED

DEC 08 2021

CONSUMER PROTECTION
DIVISION

Dear Sir or Madam:

On behalf of our client, Atalanta Corporation and other Gellert Global Group related entities (collectively “Atalanta”), a food importer headquartered at 1 Atalanta Plaza Elizabeth, NJ 07206, we provide this letter to your office as notice of a recent data security incident. By providing this notice, Atalanta does not waive any rights or defenses regarding the applicability of the Idaho’s data notification laws or personal jurisdiction.

On the morning of July 25, 2021, Atalanta detected suspicious activity in its systems. Upon becoming aware of this activity, Atalanta immediately alerted law enforcement, implemented measures to further improve the security of its systems and practices, and worked with a leading privacy and security firm to aide in its investigation and response. The investigation determined that an unauthorized individual or individuals gained access to certain Atalanta systems from July 6, 2021, until July 25, 2021, and encrypted certain Atalanta systems on July 25, 2021 (the “Incident”). As part of the extensive investigation, Atalanta was able to determine the extent of the data affected by the Incident, the number of affected individuals, and the identity of individuals on November 8, 2021.

The Incident potentially impacted 4,050 affected individuals, including two (2) Idaho residents, and is known to have impacted the following data elements: name; address; date of birth; social security number; driver’s license number; financial account number with password; passport number; individual taxpayer number; medical information; and health insurance information. Though this is an exhaustive list of the data elements, and not all potentially affected individuals had all the aforementioned data elements impacted by the Incident. Potentially affected individuals were notified of the Incident on December 8, 2021. Moreover, as Atalanta did not have contact information for all affected individuals, it notified state-wide media and posted a notification on its website on December 8, 2021. Atalanta is providing potentially affected individuals with two years of credit monitoring. A copy of the notification to affected individuals is attached hereto.

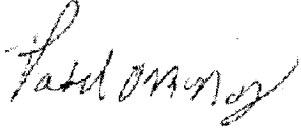
Office of the Idaho Attorney General

December 8, 2021

Page 2

Please feel free to contact me with any questions at 716-898-2102 or pmcnally@beckage.com.

Sincerely,

A handwritten signature in cursive script, appearing to read "Patrick D. McNally".

Patrick D. McNally, Esq.

Certified Information Privacy Professional, United States (CIPP/US)

Encls.

December 8, 2021

14 1 3758 *****SNGLP



Dear [REDACTED]:

On behalf of Atalanta Corporation and other Gellert Global Group entities (collectively “Atalanta” or “we”), this letter is to inform you that this past summer we experienced a data incident that potentially involved your personal information (“Information”). We are unaware of any misuse of your Information, but we wanted to provide you with information about the incident and provide steps you can take to protect your Information as a precaution.

What Happened?

On July 25, 2021, we detected suspicious activity on our network, including the encryption of certain systems (the “Incident”). Upon becoming aware of this activity, we immediately took steps to address and contain the Incident. We engaged counsel and began to remediate the situation, while simultaneously conducting a forensic investigation. The forensic investigation concluded that certain Information was accessed and acquired without authorization as result of this Incident, but there is no indication that any Information has been misused.

Why Does Atalanta Have My Information?

We collect certain Information as part of our process of onboarding and servicing current and former Atalanta employees. Additionally, as part of our business during the COVID-19 pandemic, we have collected certain Information regarding visitors to Atalanta for health and safety purposes.

What Information Was Involved?

We determined that the following types of Information may have present in the affected systems: names; addresses; dates of birth; social security numbers; driver’s license numbers; financial account numbers; passport numbers; individual taxpayer numbers; medical information; and health insurance information. Note that this list describes general categories of Information involved in this Incident, and likely includes categories that are not relevant to you.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and

security firm to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

It is always recommended that you regularly review account statements and report any suspicious activity to your financial institution. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

As an added precaution to help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorksSM. To activate your membership and start monitoring your personal information through this service, please follow the steps below:

- Ensure that you **enroll by February 28, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>; you will need to provide this **activation code**: XXXXXXXXXX

If you have questions or need assistance enrolling, please call 855-414-6049, by **February 28, 2022**. Be prepared to provide **engagement number B022325** as proof of eligibility for the identity restoration services by Experian.

For More Information.

If you have any questions about the Incident, please call 855-414-6049, Monday through Friday, from 9:00 a.m. to 5:00 p.m. and Saturday, and Sunday, from 11:00 a.m. to 8:00 p.m. Eastern (excluding some U.S. national holidays).

Sincerely,

Andrew Gellert and Thomas Gellert

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.