Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

August 31, 2021

By Electronic Mail

Office of the New Hampshire Attorney General
Consumer Protection Bureau
DOJ-CPB@doj.nh.gov

Re: Security Incident Notification

To Whom It May Concern:

I am writing on behalf of Wyandot, Inc. ("Company" or "Wyandot") to inform you of an incident that may have impacted personal information of two New Hampshire residents. Wyandot is a premier custom snack food manufacturer headquartered at 135 Wyandot Avenue, Marion, Ohio 43302.

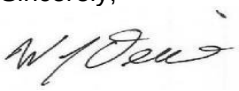
On April 4, 2021, the Company discovered that an unauthorized third-party had gained access to its systems. The Company promptly shut down its systems and engaged leading cybersecurity experts to assist with an investigation into the nature and scope of the incident. The Company also notified law enforcement. After an extensive investigation and careful review of potentially impacted systems, on July 30, 2021, the Company determined that the unauthorized third-party may have gained access to personal information maintained by the Company. At this time, the Company has identified evidence the unauthorized third-party accessed its systems on multiple occasions beginning on July 21, 2020 and ending on April 16, 2021. Wyandot is not aware of evidence indicating that the unauthorized third-party is currently able to access the Company's systems.

The information that may have been accessed includes name, address, contact information, date of birth, Social Security number, financial account number, driver's license number, credit or debit card number, health insurance information, and other health related information that may have been shared with the Company for employee benefits purposes of some current and former Company employees, beneficiaries, and applicants. After discovering the incident, the Company took steps to prevent further unauthorized access and has taken additional steps to reduce the risks of this type of incident from recurring, including resetting user credentials and deploying additional monitoring tools.

The Company sent notice by postal mail to the two New Hampshire residents on August 27, 2021. We include a sample individual notice in this notification. In addition to providing information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, the Company is offering credit monitoring and identity theft protection services for two years through Experian, at no cost to the impacted residents.

Please feel free to contact me should you have any questions or require additional information.

Sincerely,



James Denvil
Counsel
w.james.denvil@hoganlovells.com
D 1 202 637 5521

Enclosure

Wyandot, Inc.
135 Wyandot Avenue
Marion, OH 43302

August 27, 2021

G7621-L01-0000001 T00001 P001 ********SCH 5-DIGIT 32808
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to inform you of a cybersecurity incident that may have affected your personal information. This notice describes what we know, steps we have taken in response to the incident, and additional actions you may wish to take to protect yourself.

WHAT HAPPENED

On April 4, 2021, we identified suspicious activity on our systems. We promptly took steps to determine the nature and scope of the incident. Additionally, we engaged with external security experts and notified law enforcement. After an extensive investigation and review, on July 30, 2021, we determined that an unauthorized third-party accessed certain files containing some personal information collected for employment and benefits purposes. At this time, we believe that the unauthorized third-party accessed our systems on multiple occasions beginning July 21, 2020 and ending April 16, 2021. Although we are not aware of any evidence indicating that the unauthorized third-party was attempting to sell or misuse your personal information, we are notifying those that were potentially affected out of an abundance of caution.

WHAT INFORMATION WAS INVOLVED

The personal information about you that may have been accessed by the unauthorized third party may have included your name, address, contact information, date of birth, Social Security number, financial account notification, driver's license number, credit or debit card number, health insurance information, and other health related information that may have been shared with us for benefits purposes.

WHAT WE ARE DOING

We take the privacy and security of your personal information seriously. After discovering the incident, we took immediate steps to prevent future unauthorized access by investing in additional security controls and further expanding our digital monitoring capabilities. Additionally, although we are not aware of any evidence indicating that the unauthorized third party sought to sell or misuse your personal information, we have arranged for you to obtain two years of credit monitoring and identity theft protection services through Experian at no cost to you.

WHAT YOU CAN DO

We know that the privacy and security of your personal information is important to you. We encourage you to enroll and take advantage of the credit monitoring and identity theft protection services provided by Experian. Additional information about the services and enrollment instructions are included in Attachment 2 to this letter. Even if you do not choose to enroll in the program, there are other steps you can take to protect yourself. Please refer to Attachment 1 to this letter, which provides information about those steps.

FOR MORE INFORMATION

If you have any questions or need additional information, please call (844) 933-2743, Monday through Friday from 8:00 am to 10:00 pm Central Time and Saturday and Sunday from 10:00 am to 7:00 pm Central Time, excluding major U.S. holidays. Be prepared to provide your engagement number: B017912.

Sincerely,

Robert Sarlls
President and CEO

Enclosures

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://www.consumer.ftc.gov/articles/0003-phishing.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.alerts.equifax.com	www.transunion.com/fraud	www.experian.com/fraud
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft, Fraud Alerts, and security freezes and the steps you can take to protect yourself. If you are a resident of Maryland, North Carolina, Iowa, Oregon you can also reach out to your respective state's Attorney General's office at the contact information below. Residents of other states can find information on how to contact their state attorney general at www.naag.org/naag/attorneys-general/whos-my-ag.php.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

North Carolina Attorney General's Office
90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / https://ncdoj.gov/

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding Credit Freezes.

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
www.freeze.equifax.com	www.transunion.com/freeze	www.experian.com/freeze
1-800-349-9960	1-888-909-8872	1-888-397-3742

To request a Credit 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 five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)

Attachment 2: Experian Credit Monitoring and Identity Theft Services Enrollment Information

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2021** (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, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 933-2743 by November 30, 2021. Be prepared to provide engagement number B017912 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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, Equifax and Transunion files 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 933-2743. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

* 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.