ECKERT
SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

October 27, 2021

VIA FIRST CLASS MAIL

Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

This notice is provided on behalf of my client, Maumee Express Inc. ("MXI"), headquartered in Langhorne, Pennsylvania, following a data breach that may have involved the name, address, date of birth, and Social Security number of one (1) New Hampshire resident. MXI will provide written notice to this individual later today, via U.S. mail. The notice letter includes general advice on how to protect one's identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services. A copy of the notice letter is enclosed and additional information about the incident is below.

On August 16, 2021, MXI learned that a large number of emails had been sent from an MXI email account without authorization. MXI immediately launched an investigation, disabled the affected email account, and reset account passwords. MXI also engaged legal counsel with an expertise in cybersecurity. Legal counsel subsequently hired a nationally-recognized digital forensics firm to assist with the investigation so that MXI could better understand what happened, and, more importantly, help prevent something like this from happening again.

The investigation revealed that there had been incidents of unauthorized access to one MXI email account between August 10, 2021 and August 16, 2021. Because of this, and because MXI was unable to identify which specific emails may have been accessed or acquired, MXI reviewed the contents of the email box in order to determine who may have been affected, what information may have been involved and where those people reside so that it could provide proper notice. On September 8, 2021, MXI learned that the compromised email account contained personal information of one (1) New Hampshire resident.

MXI is investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. To further enhance network security and help prevent similar occurrences in the future, MXI has taken, or will be taking, the following steps:

1. Closely monitoring and restricting outside access to its systems;
2. Increasing the frequency of its password reset policy;
3. Adding two-factor authentication to access the network;
4. Strengthening spam filtering to help block dangerous emails;
5. Updating response procedures to more quickly and effectively respond to incidents;
6. Enhancing cyber training and providing regular communications in order to increase cyber awareness;
7. Updating policies to promptly terminate inactive accounts; and
8. Regularly reviewing email boxes in order to remove or archive outdated information that is no longer needed.

MXI is committed to protecting the personal information in its possession and will continue to take steps to safeguard it. Should you have any questions or concerns, please do not hesitate to contact me.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure

MXI GROUP

290 Stone Mill Road Abingdon VA 24210
276-628-1156 Fax: 276-525-4241

October 27, 2021

<<first>> <<last>>
<<street>>
<<city>>, <<state>> <<zip>>

IMPORTANT INFORMATION – PLEASE REVIEW CAREFULLY
NOTICE OF DATA SECURITY INCIDENT

Dear <<first>> <<last>>:

I am writing to tell you about a recent data security incident at Maumee Express Inc. ("MXI") that may have resulted in unauthorized access to some of the information that we maintain about our current or former employees, their relatives, and other persons associated with Maumee Express, MXI Environmental Services, and Dynamic Recycling. We are providing this notice as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering you, and suggest ways that you can help protect your information.

What Happened

On August 16, 2021, we learned that a large number of emails had been sent from an MXI email account without authorization. As soon as we learned about this, we launched an investigation to understand what happened and, more importantly, to prevent something like this from happening again. We also engaged legal counsel with an expertise in data security, who then hired a cybersecurity firm to assist with the investigation. The investigation revealed that there had been incidents of unauthorized access to one MXI email account between August 10, 2021 and August 16, 2021.

What Information Was Involved

Once we determined that there had been unauthorized access to the account, and because we could not identify what specific information may have been accessed or taken, we reviewed the contents of the email box in order to find out: (1) what information was involved, (2) who may have been affected, and (3) where those people reside so that we could provide proper notice. Based upon the investigation, the information may have included your name, date of birth, address, driver's license number or Social Security number.

What We Are Doing About It

When we discovered this incident, we immediately disabled the affected email account and had all employees reset their passwords. We also scanned our email system to detect and neutralize any potentially dangerous emails or unauthorized activity. To further enhance our security and help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Closely monitoring and restricting outside access to our systems;
2. Increasing the frequency of our password reset policy;
3. Adding two-factor authentication to access our network;
4. Strengthening our spam filtering to help block dangerous emails;
5. Updating our response procedures to more quickly and effectively respond to incidents;
6. Enhancing our cyber training and providing regular communications in order to increase cyber awareness;
7. Updating our policies to promptly terminate inactive accounts; and
8. Regularly reviewing email boxes in order to remove or archive outdated information that we no longer need.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state and federal regulators.

What You Can Do

At this time, we are not aware of any misuse of your information. However, in an abundance of caution, we recommend that you take the following preventative measures to help detect and mitigate any misuse of your information:

1. Enroll in a complimentary, one-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE™; and up to $1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.

2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

3. Report any incidents of unauthorized activity, suspicious activity or suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

If you have any questions or concerns about this incident, you may contact us at (276) 628-6636, ext. 215, Monday through Friday, 9:00 a.m. - 4:00 p.m. Eastern.

We are very sorry this incident happened and for any inconvenience you may have experienced. The privacy and security of your information is very important to us and we remain committed to protecting it.

Very truly yours,

Ronald Potter

Ronald Potter
President
Maumee Express Inc.

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

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

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Georgia, New Jersey, 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.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. 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 all three of the 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; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display

your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report 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 and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220

New York Attorney General
1-800-771-7755
http://www.ag.ny.gov/home.html

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
https://ncdoj.gov/contact-doj/
Phone: 919-716-6000

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by**: **January 20, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: **<code>**

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 **877.288.8057** by **January 20, 2022**. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian. 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 877.288.8057. 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 one year 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.