KING & SPALDING

King & Spalding LLP
1180 Peachtree Street N.E.
Atlanta, GA 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Phyllis B. Sumner
Direct Dial: +1 404 572 4799
Direct Fax: +1 404 572 5100
psumner@kslaw.com

May 26, 2022

John M. Formella, Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Breach Affecting Access USA Shipping, LLC d/b/a "MyUS"

Dear Attorney General Formella,

I write on behalf of Access USA Shipping, LLC d/b/a "MyUS" ("MyUS" or "Company") regarding a security incident.

On March 10, 2022, MyUS experienced a ransomware incident, which caused disruption to its website, mobile application, and IT systems. As soon as the Company learned of the ransomware incident, it immediately launched an investigation, retaining third party cybersecurity experts to assist in investigating the incident and remediating its systems. The experts were able to quickly contain the incident. Additionally, the Company promptly notified law enforcement.

MyUS identified some initial evidence on March 28, 2022 that some data may have been exfiltrated by the unauthorized party. As the forensic investigation continued, the Company undertook an extensive analysis of its files to determine which individuals and data may have been affected. On April 25, 2022, the Company identified certain customers whose personal information may have been affected. Although the Company was unable to confirm unauthorized acquisition of that information, starting this week MyUS will begin notifying those individuals and offering them a one-year free subscription to Experian's identity monitoring services.

Based on its investigation to date, the Company has determined that personal information in files that may have been accessed or acquired without authorization included: names, addresses, phone numbers, email addresses, dates of birth, number and/or picture of driver's license and/or other identification card, passport numbers, and social security numbers.

We have identified three (3) New Hampshire residents whose personal information as described above may have been exfiltrated in this incident. An unaddressed copy of the letter is attached. MyUS has also established a call center to answer customer questions: (833) 575-2857.

MyUS has enhanced its cybersecurity by: (i) adding additional monitoring and detection tools as safeguards against ransomware and other cyber threats; (ii) implementing a new endpoint and detection and response tool; (iii) increasing password complexity as well as resetting all

passwords for user, service, and administrator accounts; (iv) enforcing two-factor authentication on remote and email access; (v) replacing its incumbent virtual security operations center vendor with another provider; and (vi) adding 'dark web' and threat intelligence data feeds.

The Company remains committed to protecting its customers' personal information and assisting those whose personal information may have been affected by this incident. By virtue of this notice, MyUS does not waive any rights and reserves all rights under any applicable laws and regulations. Please do not hesitate to contact me if you have any questions regarding this letter.

Sincerely,

Phyllis B. Sumner

Enclosure:

Sample Notice of Data Breach for Customers

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

May 24, 2022

H9050-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 PROJECT OSPREY CUSTOMER
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to inform you about a data security incident that may have affected the privacy of some of your personal information. We want you to understand the steps we have taken to address this issue and additional steps that can be taken to protect your personal information. This letter explains the incident and offers you assistance for safeguarding your information, including complimentary credit and identity monitoring services.

What Happened
On March 10, 2022, MyUS experienced a ransomware incident, which caused disruption to its website, mobile application, and IT systems. As soon as we learned of the ransomware incident, we immediately launched an investigation, retaining third party cybersecurity experts to assist in investigating the incident and remediating our systems. The experts were able to quickly contain the incident. Additionally, MyUS promptly notified law enforcement.

We identified some initial evidence on March 28, 2022 that some data may have been exfiltrated by the unauthorized party. As the forensic investigation continued, MyUS undertook an extensive analysis of its files to determine which individuals and data may have been affected. On April 25, 2022, MyUS identified certain individuals whose personal information may have been affected. Although we were unable to confirm unauthorized acquisition of that information, we are notifying those individuals and offering them a one-year free subscription to Experian's identity monitoring services.

What Information Was Involved
Based on the investigation, we have determined that some of your personal information was contained in files that may have been accessed or acquired without authorization, including your first and last name, addresses, phone numbers, email addresses, dates of birth, number and/or picture of driver's license and/or other identification card, passport numbers, and/or social security numbers.

What We Are Doing
As discussed above, we took swift action in response to the ransomware incident by immediately launching an investigation, retaining third party cybersecurity experts to assist in investigating the incident, and remediating our systems. The experts were able to quickly contain the incident. Additionally, we promptly notified law enforcement. MyUS has also enhanced its cybersecurity by adding additional monitoring and detection tools as safeguards against ransomware and other cyber threats, as well as resetting user passwords and installing two-factor authentication on all systems.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for twelve 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 twelve 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 twelve 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 August 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- 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) 575-2857** by **August 31, 2022**. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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[TM]:** 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.

Please review the "Additional Resources" section included with this letter below. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

What You Can Do
In addition to activating Experian's® IdentityWorks℠ membership as indicated above, you can also take the following steps to safeguard your identity.

Order Your Free Credit Report
Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.
You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission Bureau of Consumer Protection
600 Pennsylvania Avenue NW Washington, DC 20580
(877) IDTHEFT (438-4338)
www.ftc.gov/idtheft

For D.C. Residents Only: Office of the Attorney General, 400 6th Street, NW, Washington DC 20001, 202-727-3400 https://oag.dc.gov/

For North Carolina Residents Only: Office of the Attorney General, 114 W Edenton St Raleigh, NC 27603, 877-566-7226 https://ncdoj.gov/

Placing a Security Freeze

Under the federal Fair Credit Reporting Act, you have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:
https://www.equifax.com/personal/credit-report-services/
https://www.experian.com/freeze/center.html
https://www.transunion.com/credit-freeze

As of April 22, 2022, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	**Online**	**Physical Mail**	**Phone Number**
Equifax	***Freeze request may be submitted via your myEquifax account, which you can create here***: https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***Mail the Equifax Freeze Request Form to***: Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 ***Form may be found here***: https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	***Freeze request may be submitted here***: https://www.experian.com/ncaconline/freeze	***Mail the request to***: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 ***Request must include:*** • Full Name	888-397-3742

		• Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	
TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here:*** https://service.transunion.com/dss/orderStep1_form.page?	***Mail the request to:*** TransUnion P.O. Box 160 Woodlyn, PA 19094 ***Request must include:*** • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert

To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your 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. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

More Information

MyUS remains committed to protecting personal information and assisting those whose personal information may have been affected by this incident. We regret any inconvenience or concern this incident may have caused. If you have any questions concerning this incident, please call the toll-free number at (833) 575-2857, Monday through Friday, 8:00 a.m.-10:00 p.m. Central Time, Saturday and Sunday 10:00 a.m.-7:00 p.m. Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number B053284.

Sincerely,

Ramesh Bulusu
Chief Executive Officer, MyUS