GIBSON DUNN

Gibson, Dunn & Crutcher LLP
2100 McKinney Avenue
Dallas, TX 75201-6912
Tel 214.698.3100
www.gibsondunn.com

Karl G. Nelson
Direct: +1 214.698.3203
Fax: +1 214.571.2945
KNelson@gibsondunn.com

December 23, 2015

Bob Ferguson
Attorney General of Washington
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Dear Attorney General:

We write on behalf of Matson Navigation Company, Inc. and Horizon Lines to notify you of a missing device containing personal information of mariners who have sailed on Matson Navigation Company and Horizon Lines ships. As of the date of this notice, we have no indication that the device has been used or was even intentionally removed.

The device was on a ship at the time it was last backed up on November 9th, 2015 while the ship was in dry dock. The ship was docked in Zhoushan, China during November. During its subsequent journey, the ship encountered rough seas, so it's possible the device was lost during this storm. The device was discovered missing on December 7th, 2015, after the ship returned to port in Tacoma, Washington.

The device contains personally identifiable information of 2,185 Washington mariners who list your state in their home address, including names, birth dates, addresses, telephone numbers, emergency contact information, and Social Security numbers, and in some (but not all) cases also including bank account and routing numbers, photocopies of passports, Transportation Worker Identification Credentials (TWIC), Merchant Mariner Documents (MMD) and Merchant Mariner Credentials (MMC), and copies of certain fit for duty medical documents. The exact date the device was lost is unknown, but appears to have been between November 9, 2015 and December 7, 2015. The database on the device was user ID and password protected, but it was not encrypted.

While we do not know with certainty if the device was stolen or lost, or if any data was accessed on the device, the fact that the device is missing presents a possibility of exposure of the mariners' personal information. When the device was first discovered as missing on or about December 7, 2015, we moved rapidly in response by notifying our IT experts and leveraging both in-house and external expertise in our investigation. We have reported the incident to law enforcement and are cooperating in their investigation. We also engaged expert third parties who specialize in responding to data exposure incidents to help address this issue. Separately, we are also notifying the affected mariners about this incident so that

they can take appropriate precautions to safeguard their personal information. We are offering the potentially impacted mariners free identity protection services and notifying them of avenues by which they may seek help from law enforcement if they believe their personal information may have been improperly used. Template copies of individual notification letters sent to mariners in your state are enclosed.

We continue to investigate the matter as well as to assess potential changes to our data systems and procedures with the goal of further enhancing their security.

For further information, you may contact Wayne A. Parker, Assistant General Counsel of Matson Navigation Company, Inc. by phone at (510) 628-4355 or by mail at 555 12th Street, Oakland, CA 94607.

Sincerely,

Karl G. Nelson

KGN/jcc
Attachments

HORIZON LINES

Processing Center • P.O. BOX 141578 • Austin, Texas 78714

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 23, 2015

Re: Data Loss Incident

Dear John Sample:

I am writing to let you know that a device containing information regarding mariners who have served aboard vessels operated by Horizon Lines has been identified as missing. While we have no indication that the device has been used or was even intentionally removed, and while accessing any information on the device requires a valid user ID and password, we take the security of such information seriously and are accordingly writing to inform you of this incident.

The device was first identified as potentially missing on or about December 7, 2015 and appears to have been lost between November 9 and December 7, 2015. While our investigation is ongoing, we have determined that among the electronic files contained on the device were ones containing individualized information of mariners who have served aboard vessels operated by Horizon Lines since the year 2000. Accordingly, we believe your personal information may have been contained on the missing device. The personal information on the device included names, birth dates, addresses, telephone numbers, emergency contact information, Social Security numbers, and in some cases bank account and routing numbers, photocopies of passports, Transportation Worker Identification Credentials (TWIC), Merchant Mariner Documents (MMD) and Merchant Mariner Credentials (MMC), and copies of certain fit for duty medical documents.

The Company has reported the incident to law enforcement and is cooperating in their investigation of the incident. Thus far, we have found no evidence to suggest that your personal information has been misused. Nevertheless, as a precautionary measure, we are reaching out to you so that you are aware of the incident and can take steps to further protect your personal information.

As an added precaution, we have arranged to have AllClear ID protect your identity for up to 12 months at no cost to you. The following identity protection services start on the date of this notice and will be available to you for registration for the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity protection and repair guidance. This service is automatically available to you at no cost. If a problem arises, simply call **1-855-711-5990 (toll free) or 1-512-201-2169 (toll)** and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at **enroll.allclearid.com** or by phone by calling **1-855-711-5990 (toll free) or 1-512-201-2169 (toll)** within the next 12 months using the following redemption code: Redemption Code. Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

In addition, you may want to consider taking some or all of the precautions described on the attached summary of "Additional Actions to Consider," which contains general guidance for protection against identity theft or fraud.

Horizon places a high value on the security of personal information, and we regret any inconvenience this may have caused. Please feel free to contact the Company by calling Danny Defanti at (510) 628-4518 or Dale MacGillivray at (510) 628-4362 if you have any questions regarding this matter.

Sincerely,

John W Sull

Captain John W. Sullivan
Vice President, Vessel Operations & Engineering

Additional Actions to Consider

Although we have not found any indication that personal information has been misused, as a precaution, you may wish to consider taking some or all of the following additional steps.

You should remain vigilant for evidence of fraud or identity theft, including by regularly reviewing your account statements and credit reports. If you discover suspicious or unusual activity on your accounts or suspect identity theft or fraud, report it immediately to your financial institutions.

If you wish to do so, you may review credit reports from each nationwide credit reporting agency. If you discover information arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your file. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by visiting www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the credit reporting agencies at:

Equifax
P.O. Box 105873
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013-2002
888-397-3742
www.experian.com

TransUnionCorp
P.O. Box 1000
Chester, PA 19022
800-680-7289
www.transunion.com

For residents of Iowa, North Carolina, and Maryland:

State laws advise you to contact your state's Attorney General to obtain information about preventing identity theft or to report any suspected identity theft.

IA Attorney General's Office
Hoover State Office Building
11305 E. Walnut Street
Des Moines, IA 50319
(800) 373-5044
www.iowaattorneygeneral.gov

MD Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6300
www.oag.state.md.us

NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
www.ncdoj.gov

In addition, you have the right to contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can contact the FTC at:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

If interested, you can also visit http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf to review an online copy of "Taking Charge: What to Do If Your Identity Is Stolen," a comprehensive guide from the FTC to help you guard against and deal with identity theft.

You also may obtain additional information from the FTC and the nationwide credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert by calling one of the nationwide credit reporting agencies listed above. When that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. A security freeze is another fraud prevention tool that prohibits anyone from accessing your credit history without your authorization. There is normally a fee for obtaining a security freeze, which is generally waived if you are a victim of identity theft. If you request a security freeze, you must unfreeze your credit file before applying for credit or other services that require accessing your credit history. You should be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of requests you make for new loans, credit mortgages, employment, housing, or other services.

For Incidents Involving Personal Health Information:

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Matson®

Processing Center • P.O. BOX 141578 • Austin, Texas 78714

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 23, 2015

Re: Data Loss Incident

Dear John Sample:

I am writing to let you know that a device containing information regarding mariners who have served aboard vessels operated by Matson Navigation Company has been identified as missing. While we have no indication that the device has been used or was even intentionally removed, and while accessing any information on the device requires a valid user ID and password, we take the security of such information seriously and are accordingly writing to inform you of this incident.

The device was first identified as potentially missing on or about December 7, 2015 and appears to have been lost between November 9 and December 7, 2015. While our investigation is ongoing, we have determined that among the electronic files contained on the device were ones containing individualized information of mariners who have served aboard vessels operated by Matson since the year 2000. Accordingly, we believe your personal information may have been contained on the missing device. The personal information on the device included names, birth dates, addresses, telephone numbers, emergency contact information, bank account and routing numbers, and Social Security numbers.

The Company has reported the incident to law enforcement and is cooperating in their investigation of the incident. Thus far, we have found no evidence to suggest that your personal information has been misused. Nevertheless, as a precautionary measure, we are reaching out to you so that you are aware of the incident and can take steps to further protect your personal information.

As an added precaution, we have arranged to have AllClear ID protect your identity for up to 12 months at no cost to you. The following identity protection services start on the date of this notice and will be available to you for registration for the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity protection repair guidance. This service is automatically available to you at no cost. If a problem arises, simply call **1-855-711-5990 (toll free) or 1-512-201-2169 (toll)** and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at **enroll.allclearid.com** or by phone by calling **1-855-711-5990 (toll free) or 1-512-201-2169 (toll)** within the next 12 months using the following redemption code: Redemption Code. Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

In addition, you may want to consider taking some or all of the precautions described on the attached summary of "Additional Actions to Consider," which contains general guidance for protection against identity theft or fraud.

Matson places a high value on the security of personal information, and we regret any inconvenience this may have caused. Please feel free to contact the Company by calling Danny Defanti at (510) 628-4518 or Dale MacGillivray at (510) 628-4362 if you have any questions regarding this matter.

Sincerely,

John W Sull

Captain John W. Sullivan
Vice President, Vessel Operations & Engineering

Additional Actions to Consider

Although we have not found any indication that personal information has been misused, as a precaution, you may wish to consider taking some or all of the following additional steps.

You should remain vigilant for evidence of fraud or identity theft, including by regularly reviewing your account statements and credit reports. If you discover suspicious or unusual activity on your accounts or suspect identity theft or fraud, report it immediately to your financial institutions.

If you wish to do so, you may review credit reports from each nationwide credit reporting agency. If you discover information arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your file. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by visiting www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the credit reporting agencies at:

Equifax
P.O. Box 105873
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013-2002
888-397-3742
www.experian.com

TransUnionCorp
P.O. Box 1000
Chester, PA 19022
800-680-7289
www.transunion.com

For residents of Iowa, North Carolina, and Maryland:

State laws advise you to contact your state's Attorney General to obtain information about preventing identity theft or to report any suspected identity theft.

IA Attorney General's Office
Hoover State Office Building
11305 E. Walnut Street
Des Moines, IA 50319
(800) 373-5044
www.iowaattorneygeneral.gov

MD Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6300
www.oag.state.md.us

NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
www.ncdoj.gov

In addition, you have the right to contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can contact the FTC at:

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

If interested, you can also visit http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf to review an online copy of "Taking Charge: What to Do If Your Identity Is Stolen," a comprehensive guide from the FTC to help you guard against and deal with identity theft.

You also may obtain additional information from the FTC and the nationwide credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert by calling one of the nationwide credit reporting agencies listed above. When that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. A security freeze is another fraud prevention tool that prohibits anyone from accessing your credit history without your authorization. There is normally a fee for obtaining a security freeze, which is generally waived if you are a victim of identity theft. If you request a security freeze, you must unfreeze your credit file before applying for credit or other services that require accessing your credit history. You should be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of requests you make for new loans, credit mortgages, employment, housing, or other services.