RE: Notice of Data Security Incident

Dear guest,

We are writing to provide information on a data security incident that has affected some Hurtigruten guests' information.

Our investigations indicate that information for a limited number of guests having booked expedition voyages with two ships, MS Fram and MS Midnatsol, in a certain time period have been affected by the incident. For MS Fram the relevant time period is from 2018 to 2020. For MS Midnatsol the relevant time period is from 2016 to 2020.

We recently learned that your information has been affected by this incident.

What happened?

On December 14, 2020, we learned that an unauthorized actor gained remote access to our network and encrypted parts of our computer systems. At that time, however, we were unable to determine which guests may have been affected, if any, and what information might have been accessed.

We immediately disabled affected computer systems, took down their internet connection to prevent any further intrusion and launched a forensic investigation to determine the nature and scope of the incident. We understand that Hurtigruten was one of many companies that was a victim of this type of intrusion.

What Information Was Involved?

Based on our investigations, we have recently determined that your affected information involves:

- Name and date of birth;
- If you were sailing with MS Midnatsol, your passport number and passport expiration date; and
- For some guests the affected information involves e-mail address, mailing address, and/or phone number

Based on our investigations to date, the unauthorized actor **did not** gain access to your credit or debit card information, social security numbers, driver's license numbers, or other government-issued identification card numbers. Hurtigruten **does not** store credit or debit card information.

What We Are Doing?

As noted above, we immediately took steps to contain the issue and commenced an investigation to determine the data and individuals that may have been affected.

We reported this matter to Norwegian law enforcement and the Norwegian Data Protection Authority (since Hurtigruten is based in Norway) and the Federal Bureau of Investigation. We also notified other applicable privacy regulatory authorities.

Over the past years we have made significant investments in data privacy and cyber security. Since this incident, we have further strengthened these efforts and our internal experts are working closely with third-party cybersecurity experts to further enhance the security of our systems and reduce the risk of a similar event happening in the future.

What Can You Do

On February 18, 2021, we discovered the unauthorized actor placed some of the above information on a difficult to access part of the web. We do not have any indication of actual harm to affected individuals as a result of this

incident, but we still recommend you follow the enclosed additional steps that you can take to protect your personal information.

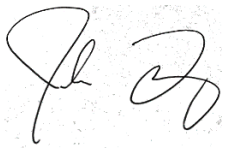
We sincerely regret any concerns or inconvenience that this incident may cause you.

For More Information

As a California resident, please contact us at the following number to process your identity theft protection:

Phone: 1 (833) 907-3030 (toll-free number). The phone line is open between 6:00 a.m. to 6:00 p.m. PST, Monday through Friday, excluding major U.S. holidays.

Sincerely,



John Downey

President, Hurtigruten Americas

California Information about Identity Theft Protection

Monitor Your Accounts. As a precautionary measure, we recommend that you remain vigilant by regularly reviewing statements from your accounts and periodically obtaining your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, or by calling toll-free 1-877-322-8228, or by mailing to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alerts. You have the right to place a fraud alert on your credit report at no cost. An initial fraud alert lasts one year and is placed on your 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. Should you wish to place a fraud alert, please contact any one of the agencies listed above. Additional information is available atwww.annualcreditreport.com.

Credit Freeze. You have the right to put a security freeze, also known as a credit freeze, on your credit file, for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. As a result, using a credit freeze may delay your ability to obtain credit. In order to place a credit freeze, you may be required to provide the consumer reporting agency with your personal information including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. Should you wish to place a credit freeze, please contact each of the three major consumer reporting agencies listed above separately.

Monitor Your Personal Health Information. If applicable to your situation, 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 California Office of Privacy Protection at www.oag.ca.gov/privacy for additional information.

Additional Information. You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your State's Attorney General or the Federal Trade Commission (FTC). Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. Contact information for the FTC is: **The Federal Trade Commission**, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-4338, www.ftc.gov/idtheft.