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.

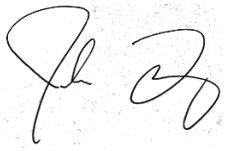
For More Information

If you have questions or require further assistance, please contact us via one of these channels:

Website: https://www.hurtigruten.com/info/

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

Additional Guidance

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent institution or any suspected incidence of identity theft to law enforcement authorities.

Obtain a Copy of Your Credit Report

Order a copy of your credit report from both Equifax Canada and TransUnion Canada. Each credit bureau may have different information about how you have used credit in the past. Ordering your own credit report has no effect on your credit score. Equifax Canada refers to your credit report as "credit file disclosure". TransUnion Canada refers to your credit report as "consumer disclosure". You can make the request by contacting the two credit bureaus as indicated below. You will need to follow the instructions provided and also confirm your identity by providing identification or answering a series of questions.

	Equifax	**TransUnion**
By mail or fax	National Consumer Relations P.O. Box 190, Station Jean Talon Montreal, Quebec H1S 2Z2 or by fax to: 514-355-8502	CONSUMER RELATIONS CENTRE 3115 Harvester Road, Suite 201 Burlington, Ontario L7N 3N8
By telephone	1-800-465-7166	Tel: 1-800-663-9980 (except Quebec) Tel: 1-877-713-3393 (Quebec residents)
Online	https://www.consumer.equifax.ca/personal/	https://www.transunion.ca/product/credit-report

Place a Fraud Alert on Your Credit Report

You can also place a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax Canada and TransUnion Canada using the information above.