MAYER | BROWN

Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006-1101
United States of America

T: +1 202 263 3000
F: +1 202 263 3300

mayerbrown.com

RECEIVED
JUL 07 2021
CONSUMER PROTECTION

David Simon
Partner
T: +1 202 263 3388
F: +1 202 263 5371
dsimon@mayerbrown.com

CONFIDENTIAL TREATMENT REQUESTED

July 2, 2021

BY MAIL

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

Re: Virgin Cruises Intermediate Limited – Notification of Incident

Dear Attorney General Formella:

In accordance with New Hampshire Revised Statute § 359-C:20, we write on behalf of our client, Virgin Cruises Intermediate Limited ("Virgin Voyages"), to inform you that the personal information of three (3) New Hampshire residents may have been accessed and acquired without authorization as part of a data security incident.

On February 1, 2021, Virgin Voyages became aware of unauthorized access to certain Virgin Voyages IT system logging data. Upon learning of the incident, Virgin Voyages promptly commenced an investigation, engaged a leading cybersecurity firm to assist in assessing the scope of the potential incident, and took steps to terminate the unauthorized access. During the course of the investigation, it became apparent that certain data affected by the incident contained personal information relating to individuals. At this time, Virgin Voyages has no knowledge that any personal information has been used improperly.

Virgin Voyages' investigation has revealed that the data may have included certain individuals' personal information, including government-issued identification numbers and physical condition. Pursuant to New Hampshire Revised Statute § 359-C:20, any business with a reasonable belief that personal information was acquired by an unauthorized individual or entity must provide notification to each affected New Hampshire resident. Virgin Voyages will distribute notification letters to all impacted individuals on July 6, 2021. A copy of this notice is attached.

Under New Hampshire Revised Statute § 359-C:20, any business with a reasonable belief that personal information was acquired by an unauthorized individual or entity must report the unauthorized breach to the New Hampshire attorney general's office. Accordingly, we are writing to notify you of this incident as we and Virgin Voyages are committed to working with you to address any questions you may have.

Virgin Voyages has engaged a leading cybersecurity firm to support its investigation and is taking additional security steps to help prevent future incidents. Further, Virgin Voyages has

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian partnership).

provided individuals with information about steps they can take to protect themselves from identity theft or fraud.

We assure you that Virgin Voyages takes this incident and the privacy and security of personal information in its care seriously. Should you have any questions or require further information, please do not hesitate to contact me.

Sincerely,

David Simon
Partner

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

July 6, 2021

G5882-L01-0000001 T00001 P001 ********SCH 5-DIGIT 32808
SAMPLE A. SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Notice of Data Breach

Dear Sample A. Sample:

We are writing to tell you about a data security incident that may have affected some of your personal information. We are providing you with information about the incident and steps that you may take to protect against the possibility of identity theft and fraud, should you feel it necessary to do so.

What happened?

In early February, we became aware of unauthorized access to certain Virgin Cruises Intermediate Limited ("Virgin Voyages") IT system logging data. We promptly commenced an investigation, engaged a leading cybersecurity firm to assist in assessing the scope of the potential incident, and took steps to terminate the unauthorized access. During the course of our investigation, it became apparent that certain data affected by the incident contained personal information relating to individuals. As part of our ongoing investigation, we have determined that certain personal data about you may have been subject to unauthorized access during the incident. At this time, we have no knowledge that any of your information has been used improperly.

What information was involved?

The information involved may have included a government-issued identification number and/or physical conditions, if you provided any such information to Virgin Voyages.

What we are doing?

We take the security of personal information in our care seriously. We have engaged a leading cybersecurity firm to support our investigation and are taking additional security steps to help prevent future incidents.

What you can do.

We understand you may have concerns about this incident. We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, 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.

We sincerely regret this incident and any inconvenience or concern it may cause you. Should you have questions or concerns regarding this matter, please contact us by email at dataincident@virginvoyages.com, by phone at (954) 358-3976, or by mail at 1000 South Pine Island Road, Suite 600, Plantation, Florida 33324.

Sincerely,

Virgin Voyages Team

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. The credit reporting agencies can also provide information about fraud alerts and security freezes.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Maryland, Puerto Rico, 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 to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit a written request to any of the three 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 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft, including the use of fraud alerts and security freezes.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Residents of Maryland, North Carolina, New York, Connecticut, and the District of Columbia can obtain more information about preventing and avoiding identity theft from their Attorneys General using the contact information below.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 202-727-3400, https://oag.dc.gov/about-oag/contact-us.

Reporting of identity theft

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission, and the Oregon Attorney General.