Freshfields Bruckhaus Deringer US LLP

PETER JAFFE
700 13th Street, NW
10th Floor
Washington, DC 20005-3960
Tel +1 202 777 4551
peter.jaffe@freshfields.com

Via U.S. Mail

June 22, 2021

Office of the Attorney General

33 Capitol Street

Concord, NH 03301

To the Office of the Attorney General:

We write to inform you that Royal Caribbean Group ("RCL") will be sending notices to New Hampshire residents advising them of a data incident. On February 12, 2021, RCL became aware that a malicious actor had gained access to a limited number of employee email accounts as part of a phishing attack. A subsequent prioritized review of the contents of those accounts identified some personal data potentially giving rise to a notification obligation under New Hampshire law. At this time, RCL has identified 62 such records for which the corresponding person appears to be a New Hampshire resident.

Although the personal information identified for this population varies from individual to individual, in general such information may include names, dates of birth, gender, nationality, contact information, passport number, and/or state identification number. For RCL employees, the information may include data such as position title and voyages on which crewmembers served. For RCL guests, the information may include data about the guest's vacations with RCL, such as destinations visited.

We are not currently aware of any financial harm to any New Hampshire residents whose data was involved in this incident.

Starting on June 22, formal notices of the incident will be sent by U.S. mail to guests for whom we have identified a New Hampshire mailing address. We are also working to notify New Hampshire employees and other individuals as promptly as possible.[1] A copy of the anticipated notice for guests is attached.

RCL takes the security of information on guests, employees, and others seriously. We continue to evolve our cyber security practices in line with our business's reliance on technology and the changing external threat landscape. Since this attack, RCL has taken additional steps to prevent this type of incident in the future. This includes further actions to enhance our controls and train our employees in order to safeguard personal information.

Please contact me if you have any questions.

Sincerely,

Peter Jaffe

Enclosures (1)

---

[1] In searching for mailing addresses, RCL consulted data involved in the incident and also sought to identify corresponding mailing information in its company databases.

Royal Caribbean Group
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

We are writing to let you know about an incident in which a third party may have gained unauthorized access to your personal information. Below is a summary of what happened, what personal data was involved, what we are doing, what you can do, and where you can obtain more information.

Notice of Data Breach	
What happened?	At some time between February 6, 2021 and February 18, 2021, your personal data may have been accessed by a third party who gained unauthorized access to a limited number of our employees' email accounts. Upon discovery, we immediately secured the email accounts, began an investigation, and arranged resources to start identifying, informing, and assisting persons whose personal information may have been involved. During our review, we identified your information as having potentially been accessed, although we are not aware of any attempt to exploit this incident in a malicious way.
What personal data was involved?	In addition to your name, certain internal identifiers that we use, and information about your vacations with a Royal Caribbean brand, the personal data that may have been accessed includes some or all of the following: your contact information, date of birth; gender; nationality; passport number; state driver's license or other government identification number; and/or tokenized or partial payment card information (that is, payment card numbers that have been redacted or replaced with a placeholder to prevent misuse). To our knowledge, your information did not include your full, unencrypted payment card information, or social security number or equivalent taxpayer identifier. Therefore, we believe the risk of someone misusing your data is low.
What are we doing?	We are taking this incident very seriously and have taken steps to strengthen our protection of personal information, including updating email access controls. We have not identified any further unauthorized activity since the breach was identified and contained in mid-February. We will continue to closely monitor and take further steps as appropriate to safeguard your personal data.
What can you do?	Although we are not aware of any attempts to exploit this incident in a malicious way, and although we believe the risk of someone misusing your data is low, third parties involved in the incident could attempt to use your personal information to take fraudulent actions. To reduce your risk of being subject to identity theft, you can monitor your financial accounts and your account statements for unusual or unauthorized activity over the next 12 to 24 months and promptly report any suspected identity theft to the police. You should be vigilant against possible "phishing" communications and emails that appear to be (but are not) sent from Royal Caribbean brand email addresses.

For more information.	We are sorry that this occurred. You can find more information about steps that you can take in the appendix to this letter. If you have any questions, please call +1 855-535-1847 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Yours sincerely,

R. Alexander Lake
Chief Legal Officer

APPENDIX

Measures that you can take to protect yourself with regard to consumer credit reporting bureaus:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

1. prevent you from getting your free annual credit report;
2. keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;
3. prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

Equifax

Fraud Alerts

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
888-836-6351 (automated service line)
800-525-6285 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Security Freezes

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
888-298-0045 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Credit Reports

Equifax Information Services LLC
P.O. Box 740241
Atlanta, GA 30374-0241
866-349-5191
https://www.annualcreditreport.com/index.action

Experian

Fraud Alerts

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.experian.com/fraud/center.html

Security Freezes

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013 (regular mail)

Experian
711 Experian Parkway
Allen, TX 75013 (overnight mail)

1-888-397-3742
https://www.experian.com/freeze/center.html

Credit Reports

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.annualcreditreport.com/index.action

TransUnion

Fraud Alerts

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://fraud.transunion.com

Security Freezes

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://freeze.transunion.com/

Credit Reports

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
800-888-4213
https://www.annualcreditreport.com/index.action

Information and assistance that you can obtain from federal and state law enforcement and consumer protection agencies: If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

Protections of the Federal Fair Credit Reporting Act
The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.*

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See www.ftc.gov/credit for additional information.*

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures.*

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).*

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. *For more information, visit www.ftc.gov/credit.*

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a resident of certain states, you have additional rights:

Massachusetts
Under Massachusetts state law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Oregon
You can reach the Attorney General of the State of Oregon at 1-877-877-9392 or by mail at help@oregonconsumer.gov.

Rhode Island
You can reach the Attorney General of the State of Rhode Island by phone at (401) 274-4400 or online at www.riag.ri.gov.

Maryland
You may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 1-410-576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General by mail at:

Identity Theft Unit
Office of the Attorney General
200 St. Paul Place
25th Floor
Baltimore, MD 21202

North Carolina
You can reach the Attorney General of the State of North Carolina by mail at:

9001 Mail Service Center
Raleigh, NC 27699-9001
+1 (919) 716-6400
http://www.ncdoj.gov