Orrick, Herrington & Sutcliffe LLP
701 Fifth Avenue
Suite 5600
Seattle, WA 98104-7097

+1 206 839 4300
orrick.com

Aravind Swaminathan

E aswaminathan@orrick.com
D +1 206 839 4340
F +1 206 839 4301

March 2, 2020

To: State Attorney General and Consumer Protection Office Distribution List

RE: Data Breach Notification

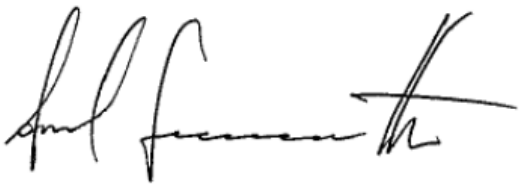
Dear Sir or Madam:

Carnival Corporation & PLC ("Carnival," "Company," "we," "us," and/or "our") is a travel leisure company. In late May 2019, we became aware of suspicious activity involving the Office 365 email systems of certain of our brands, including Carnival Cruise Line, Cunard North America, Holland America Line, Holland America Princess, Princess Cruises, P&O Cruises Australia, and Seabourn. Upon identifying this potential security issue, an investigation was commenced, with the assistance of third-party cybersecurity forensic experts to determine what happened and what data may have been impacted. It now appears that between April 11 and July 23, 2019, an unsanctioned third party gained unauthorized access to some Carnival employee and crew email accounts. Due to this access, personal information belonging to residents of your state may have been accessed without authorization, including name, address, Social Security number, government identification information, such as passport number or driver's license number, credit card and financial account information, and health-related information. Please see Exhibit A for the total number of state residents potentially impacted by this incident. Carnival is taking steps to enhance protections of our email systems, including implementing multi-factor authentication and other privacy and security controls, policies and procedures to help reduce the likelihood of such incidents occurring in the future. Carnival has also notified law enforcement of this incident and offered our full cooperation.

Notice of the incident was posted on our Holland America Line and Princess Cruises websites, and a press release was disseminated, on March 2, 2020. Notices will be mailed to consumers for whom we had up-to-date mailing information beginning the week of March 2, 2020. The notices will be customized by company and a sample of the notice to be sent to customers is attached hereto as Exhibit B. Carnival is offering free credit monitoring and identity theft protection services through ID Experts for affected individuals. Carnival is also providing contact information for recipients who have questions, instructions on how they can sign up for credit monitoring, and additional steps they can take to protect themselves.

If your office requires any further information in this matter, please contact me at +1 (206) 839-4340 or aswaminathan@orrick.com.

Sincerely,



Aravind Swaminathan
Attorney for Carnival Corporation & PLC

Exhibit A

Approximate number of potentially affected residents in Washington: 11,346

Exhibit B

Sample Consumer Notification Letter

[Logo Customized by Company]

[Mailing Date], 2020

[Recipient name]
[Recipient street address]
[Recipient state and ZIP]

NOTICE OF POTENTIAL DATA BREACH

We wanted to make you aware of a security event at [Company].

What Happened?

In late May 2019, we identified suspicious activity on our network. Upon identifying this potential security issue, we engaged cybersecurity forensic experts and initiated an investigation to determine what happened, what data was affected, and who was impacted. It now appears that between April 11 and July 23, 2019, an unsanctioned third party gained unauthorized access to some employee email accounts that contained personal information regarding our guests.

What Information Was Involved?

The types of data potentially impacted varies by guest but can include: name, address, Social Security number, government identification number, such as passport number or driver's license number, credit card and financial account information, and health-related information. This list is not specific to each guest. We do not have any evidence of misuse of the personal information affecting any individual. But, if you want to find out what of your personal data was affected, please contact us at the number provided below.

What We Are Doing.

In addition to our ongoing investigation, we reported this matter to law enforcement and are offering our full cooperation. As part of our regular process, we are undertaking a review of our security policies and procedures and implementing changes to enhance our security program. We take privacy and security of personal information very seriously, and we are offering affected individuals free credit monitoring and identity theft detection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. To enroll in the free MyIDCare services, call +1 (833) 719-0091 (toll-free U.S.) Monday through Friday from 6am to 6pm Pacific Time or visit https://app.myidcare.com/account-creation/protect and use the Enrollment Code provided above. Please note the deadline to enroll is June 1, 2020.

What You Can Do.

In addition to enrolling in the free credit monitoring and identity theft protection services being offered, we encourage you to consider taking the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- While we have no reason to suspect that your information is being misused, if you ever suspect that you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement. In addition, you may contact the FTC or your state attorney general to learn more about the steps you can take to protect yourself against identity theft. The attachment following this letter has more information about steps you can take to protect yourself against identity theft or fraud.
- Be alert for "phishing" emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, Social Security numbers, or bank account information. We do not ask for this type of sensitive information over email.

For More Information.

We sincerely regret this occurred and for any concern that this may have caused you. We take very seriously our commitment to privacy and data security. Should you have questions, or if you would like to discuss the matter further, please contact us at +1 (833) 719-0091 (toll-free U.S.).

Sincerely,

Jennifer Garone
Data Protection Officer

Attachments

Attachment A

HOW TO SIGN UP FOR MYIDCARE

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact us at +1 (833) 719-0091 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call +1 (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or to report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Attachment B

ADDITIONAL INFORMATION TO PROTECT YOURSELF

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

Consider contacting the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 +1 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 +1 (800) 680-7289 www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; +1 (888) 743-0023; or www.oag.state.md.us.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.