



July 23, 2021

By Form

Washington State Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98501

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

RE: Notice of IT Security Event Relating to Washington Residents

Dear Attorney General:

On December 25, 2020, Carnival Corporation detected unauthorized third-party access to portions of the company's information technology systems. Carnival acted quickly to shut down the event, restore operations, and prevent further unauthorized access. Additionally, an investigation was immediately commenced with assistance from leading cybersecurity forensics experts to determine what happened and what information was affected. Carnival also notified law enforcement about the incident.

On June 25, 2021, Carnival determined that the affected systems contained unencrypted personal information for a Washington resident. Carnival subsequently identified a total of three Washington residents whose personal information was impacted. The information impacted could include data routinely collected in connection with the guest travel and booking process or through the course of employment. That information may generally include names, addresses, phone numbers, passport numbers, and dates of birth. At this time, there is no evidence of any misuse of personal data, and there is no evidence of personal online credentials being impacted as a result of this event.

As part of its ongoing operations, Carnival is continuing to review security and privacy policies and procedures and implementing changes when needed to enhance information security and privacy controls. Carnival began notifying Washington residents on July 23, 2021 and is offering one year of free credit monitoring and identity theft detection services to those whose personal information may have been impacted.

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

Washington Attorney General

July 23, 2021

Page 2

Sincerely,

A handwritten signature in black ink, appearing to read 'AS', written in a cursive style.

Aravind Swaminathan

Partner

Orrick, Herrington, & Sutcliffe, LLP

<Return Name>
<Return Address>
<City> <State> <Zip>



<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

July 23, 2021

Notice of Data Breach

Dear [name],

As a valued member of the Costa family, we wanted to update you about an IT security event. We previously posted information about this event on our website on March 19, 2021. As detailed in our post, we have been working to identify the individuals whose personal information may have been impacted by this event. We are directly notifying you because your personal information has been found during that process.

What Happened?

On December 25, 2020, we detected unauthorized third-party access to portions of our information technology systems. We acted quickly to shut down the unauthorized access, restore operations, and prevent further unauthorized access. A major cybersecurity firm was engaged to investigate the matter and we notified law enforcement agencies and appropriate regulators of the event.

What Information Was Involved?

There is evidence that an unauthorized third-party gained access to certain systems, some of which may contain personal data relating to some of our guests, employees, and crew. The information impacted could include data routinely collected in connection with the guest travel and booking process or through the course of employment. That information may generally include names, addresses, phone numbers, passport numbers, and dates of birth. At this time, there is no evidence of any misuse of personal data, and there is no evidence of personal online credentials being impacted as a result of this event.

What We Are Doing.

As part of our ongoing operations, we are reviewing security and privacy policies and procedures and implementing changes to enhance information security and data protection controls.

We are also offering individuals whose personal information may have been impacted free credit monitoring and identity theft detection services for 12 months. Details on how to access these services are in the enclosed Appendix A.

What You Can Do.

Although we do not have evidence of misuse of your personal data in connection with this event, it is always a good idea to remain vigilant against threats of identity theft. Given the nature of the data breach, there are steps you can take to protect yourself:

- Regularly reviewing and monitoring your account statements for any signs of unauthorized transactions or activity.
- It is also always a good idea to be alert for “phishing” emails by someone who acts like they know you and asks you to click on a link or requests sensitive information over email.
- Changing your passwords, particularly for email and other online accounts, and enabling multi-factor authentication where possible.
- If you believe you are a victim of identity theft, reporting this to local police, asking for a police report or reference number, then contacting your financial institution to tell them what happened.

More information on these and other steps you can take are in the attached Appendix A. Please note that, in connection with the above mentioned event, Costa Cruises will not contact you by telephone or by email to ask you for any personal information including your online credentials or any financial information such as credit card numbers.

For More Information.

If you have any questions regarding this event, please contact us via email at informationdesk@costa.it.

Sincerely,



Cristina Porcelli
General Counsel

Appendix A – Information for U.S. Residents

CREDIT MONITORING

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring* services at no charge. These services provide you with alerts for one year from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Credit Monitoring* will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud, as well as a \$1,000,000 insurance reimbursement policy.

HOW DO I ENROLL FOR THE FREE SERVICES?

To enroll in Credit Monitoring* services at no charge, please log on to <www.xxx.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <CODE HERE>

In order for you to receive the monitoring services described above, you must enroll within one year from the date of this letter.

If you have questions about the incident, or want to discuss the matter further, please contact us by emailing informationdesk@costa.it. If you have any questions about enrolling in the Credit Monitoring* services, please call the U.S. toll-free number 1-866-204-1396 between the hours of 8 a.m. to 5 p.m. Eastern Time (ET), Monday through Friday.

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft, or other financial loss, you should always 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 can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission (FTC). 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 from the U.S. at +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact any one of 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 (5) 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 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; by telephone at +1 (877) 382-4357; or at 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 the Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; by telephone at +1 (515) 281-5164; or at www.iowaattorneygeneral.gov.

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

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

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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.

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

Oregon Residents: The Attorney General can be contacted at the Oregon Department of Justice, 1162 Court Street NE, Salem, Oregon 97301-4096; by telephone at +1 (877) 877-9332 (toll-free in Oregon) and +1 (503) 378-4400; or at www.doj.state.or.us.

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

* Services marked with an asterisk (*) require an internet connection and e-mail account and may not be available to minors under 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.