

UPDATE

- [Get important information on a privacy event that may impact you.](#)
- [Stay updated on current Health and Sailings Advisories.](#)

hide 

Home > Substitute Notice of Data Breach

Share

Print

SUBSTITUTE NOTICE OF DATA BREACH

Carnival Cruise Line: October 13, 2020

SUBSTITUTE NOTICE OF DATA BREACH

As a valued member of the Carnival Cruise Line family, we wanted to update you about a recent cyber event. We previously posted about this event on Carnival Corporation & plc's website on August 17, 2020.

What Happened?

On August 15, 2020, we detected unauthorized third-party access to portions of the company's information technology systems. We acted quickly to shut down the intrusion, restore operations, and prevent further unauthorized access. We also engaged a major cybersecurity firm to investigate the matter and notified law enforcement and appropriate regulators of the event.

What Information Was Involved?

While the investigation is ongoing, early indications are that in early August an unauthorized third-party gained access to certain personal information relating to some of our guests, employees, and crew. For individuals who sailed with us, the information impacted may include the data routinely collected during the guest travel booking process, during the casino experience, or at the time of employment. That information may include names, addresses, phone numbers, passport numbers, and dates of birth. The investigation into the specific data impacted is ongoing, but in some limited instances, we anticipate additional information impacted may include data such as Social Security numbers, health information, or other personal information.

Working with our cybersecurity consultants, we took steps to recover our files and have evidence indicating a low likelihood of the data being misused.

What We Are Doing

We are working as quickly as possible to identify the guests, employees, crew and other individuals whose information may have been impacted. We expect to complete this process within the next 30-60 days and will then send notifications to potentially affected individuals whose current contact information is available to the company. Along with those individual notices, affected individuals will be offered complimentary credit monitoring, as appropriate.

Meanwhile, we have issued a news release, posted website notices, and established a dedicated call center to answer questions regarding the event. When the investigation is complete, callers may confirm whether or not their information was affected. The call center is available toll-free in the U.S. at +1. 888.905.0687, 9 a.m. to 9 p.m. Eastern Time (ET), Monday through Friday.

Individuals outside the U.S. may email questions to cruisedataevent@cyberscout.com, and request that a call center representative respond back by phone.

As part of our ongoing operations, we are continuing to review security and privacy policies and procedures and implementing changes when needed to enhance information security and privacy controls.

What You Can Do

It is always a good idea to remain vigilant against threats of identity theft or fraud. You can do this by regularly reviewing and monitoring 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 can contact your local police.

It is also always a good idea to 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 financial account information.

For additional information about how to protect yourself, you may click on the below links:

- [Resources for Australian residents](#)
- [Resources for Canadian residents](#)
- [Resources for U.K. residents](#)
- [Resources for U.S. residents](#)
- [Resources for residents of other countries](#)

For More Information

If you have questions, or if you would like to discuss the matter further, please contact us at the U.S. toll-free number +1-888-905-0687 between the hours of 9 a.m. to 9 p.m. Eastern Time (ET), Monday through Friday. Individuals outside the U.S. may email questions to cruisedataevent@cyberscout.com, as well as request that a call center representative respond back by phone.

Sincerely,
Jennifer Garone
Director, Data Privacy

APPENDIX A – INFORMATION FOR AUSTRALIAN RESIDENTS

[▲Top](#)

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below is information about steps you can take to place a fraud alert or security freeze and check your credit report (where they are available). If you believe you are a victim of fraud or identity theft, you should contact your local law enforcement agency and bank. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A CREDIT REPORT

We recommend you obtain a copy of your credit report to check that it is accurate. Your credit report will show you any organisations that have recently checked your credit history. If there are any suspicious credit checks, you can contact those organisations to stop them from authorising any new accounts in your name. You are entitled to access your credit report once every 12 months for free from:

- [Equifax](#) [🔗](#), phone 138 332
- [Experian](#) [🔗](#), phone 1300 783 684
- [Illion](#) [🔗](#), phone 1300 734 806

If you suspect fraud you can contact all these credit reporting bodies (i.e. as listed above) to request a ban on your credit report, free of charge. During the ban period (of 21 days from your request but which can be extended), the credit reporting body will not disclose your consumer credit report without your written consent (or as required by law or a court/tribunal order). If a fraudster attempts to access credit by impersonating you, the credit provider (e.g. a bank) will ask the credit reporting body for a copy of your consumer credit report and

the credit reporting body will alert them to the ban you have requested and that the activity is fraudulent. This helps to protect you from fraud.

For more information, please consult the Office of the Australian Information Commissioner’s advice. [↗](#)

INFORMATION ON REDUCING THE RISK OF HARM TO YOU

Given the nature of the data breach, there are steps you can take to protect yourself and reduce your risk of harm, including:

- changing your passwords, particularly for email and internet banking accounts, and enabling multi-factor authentication;
- monitoring your banking transactions online or using paper account statements to check for any fraudulent transactions;
- for any government-issued identity document information, contacting the agency that issued the identity document for information on what steps you should take;
- for information about your tax file number, contacting the Australian Taxation Office [↗](#); and
- if you believe you are a victim of identity fraud, reporting this to local police, asking for a police report or reference number, then contacting your financial institution to tell them what happened.

For further information please consult the Office of the Australian Information Commissioner’s tips and advice. [↗](#)

INFORMATION ON IMPLEMENTING A FRAUD ALERT

You may also be able to place a fraud alert on your credit report or with your bank. 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 generally 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.

SEEKING SUPPORT

If this data breach causes you to suffer any distress, consider reaching out to family or friends or one of the support services below (as appropriate) for help.

Organisation	Help offered	Contact details
beyondblue ↗	Information and support for anxiety and depression	Phone: 1300 224 636 Chat online every day from 3 p.m. to 12 a.m. (AEST), or email ↗ any time
IDCARE ↗	Australia’s national identity and cyber support service. They can connect you with a specialist identity and cyber security counsellor.	Phone: 1300 IDCARE (432273)
Kids Helpline ↗	Support for young people any time and for any reason	Phone: 1800 55 1800 You can also chat with a web counsellor ↗ from 12 p.m. to 10

		p.m. (AEST) on weekdays and 10 a.m. to 10 p.m. (AEST) on weekends, or email a Kids Helpline counsellor any time.
Lifeline ☞	Personal crisis support	Phone: 13 11 14 Lifeline’s online chat service ☞ is available every night

APPENDIX B – INFORMATION FOR CANADIAN RESIDENTS

[▲Top](#)

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below are the names and contact information for Canadian consumer reporting agencies and additional information about steps you can take to obtain a free credit report and place a fraud alert on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local police.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

You are entitled a free copy of your credit report from each of Equifax Canada and TransUnion Canada. You can order your credit report online, by mail or by telephone. If requesting your credit report by mail, please visit the Equifax Canada and TransUnion Canada websites for the required form and information about the identity verification documents you will need.

Equifax Canada

National Consumer Relations
P.O. Box 190, Station Jean Talon
Montreal Quebec
H1S 2Z2
+1 (800) 465-7166
[Equifax website](#) [☞](#)

TransUnion Canada

Consumer Relations
3115 Harvester Road
Suite 201
Burlington Ontario
L7N3N8
+1 (800) 663-9980
[TransUnion Canada website](#) [☞](#)

INFORMATION ON IMPLEMENTING AN IDENTITY OR FRAUD ALERT

Equifax Canada and TransUnion Canada also offer fraud alert services for a fee. If you live in Ontario or Manitoba, this alert requires lenders and creditors to take reasonable steps to verify that the person involved in the transaction is you. If you live elsewhere in Canada, lenders and creditors are encouraged to contact you before extending credit but are not legally required to do so. Although this may cause a short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

APPENDIX C – INFORMATION FOR U.K. RESIDENTS

ADDITIONAL INFORMATION

To protect yourself against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below is information about steps you can take to protect yourself against the possible consequences of a data breach. If you believe you are a victim of fraud or identity theft, you should contact your local law enforcement agency and bank as soon as possible. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A CREDIT REPORT

We recommend you obtain a copy of your credit report from a credit reference agency ("CRA") to check that it is accurate. Your credit report may show credit searches or accounts you did not apply for. If there are any suspicious credit applications, you can query those directly to the organisations who have made them, or you can ask a CRA to query them to such organisations on your behalf.

You are entitled to access your statutory credit report free of charge from the three CRAs listed below:

- Equifax [🔗](#), phone 08000 850 650
- Experian [🔗](#), phone 0115 828 6738
- Illion [🔗](#), phone 0330 024 7574

For more information on CRAs, please consult the following guidance at the Information Commissioner's website. [🔗](#)

PROTECTIVE REGISTRATION

If you are a victim of (or believe to be at risk of) identity fraud, you can apply for Protection Registration at Cifas (the UK's leading fraud prevention service). This will place a flag alongside your name and personal details in the National Fraud Database, which will reduce the risk of fraudsters using your details online. Please note that this will not affect your credit score.

For more information on CRAs, please consult the following guidance at the Cifas' website. [🔗](#)

INFORMATION ON IMPLEMENTING A FRAUD ALERT

You may also be able to place a fraud alert on your credit report with your bank. 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 generally 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.

INFORMATION ON REDUCING THE RISK OF HARM TO YOU

Given the nature of the data breach there are steps you can take to protect yourself and reduce your risk of harm, including:

- changing your passwords, particularly for email and internet banking accounts, and enabling multi-factor authentication;
- monitoring your banking transactions online or using paper account statements to check for any fraudulent transactions;
- for any government-issued identity document information, contacting the agency that issued the identity document for information on what steps you should take;
- consulting the National Cyber Security Centre guidelines on cybersecurity, which you can find at the National Cyber Security Centre's website. [🔗](#)
- consulting the Get Safe Online guidelines on how to protect yourself and your devices, which you can find at the Get Safe Online website. [🔗](#)
- if you believe you are a victim of identity fraud, reporting this:

- to the local police, asking for a police report or reference number then contacting your financial institution to tell them what happened, and
- to Action Fraud, the UK's national reporting centre for fraud and cybercrime, using the [Action Fraud website](#). [↗](#)
- if you would prefer not to speak to the police, please visit the [Metropolitan Police website](#) [↗](#) for a list of alternative organisations that can provide support in relation to cyber incidents.

For further information on the risks of identity theft please consult the Information Commissioner's Office tips and advice. [↗](#)

SEEKING SUPPORT

If this data breach causes you to suffer any distress, consider reaching out to family or friends or one of the support services below (as appropriate) for help.

Organisation	Help offered	Contact details
Victim Support ↗	Support for people affected by crime and traumatic incidents.	Phone: 08 08 16 89 111 Email ↗
Mind ↗	Advice and support to empower anyone dealing with mental health issues and distress.	Phone: 0300 123 3393

APPENDIX D – INFORMATION FOR U.S. RESIDENTS

[▲Top](#)

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and 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. 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 the [Annual Credit Report website](#) [↗](#) or call toll-free at +1 (877) 322-8228.




INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact 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:

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

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; +1 (877) 382-4357; or by visiting the [FTC website](#). 


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 website](#)  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, or by visiting the [Iowa Attorney General website](#). 

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, +1 (502) 696-5300, or by visiting the [Kentucky Attorney General website](#). 

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 by visiting the [Maryland Attorney General website](#). 

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, NC 27699-9001; +1 (919) 716-6400; or by visiting [North Carolina Attorney General website](#). 

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 read the [Fair Credit Reporting PDF](#)  or visit the [FTC website](#). 

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9332 (toll-free in Oregon), +1 (503) 378-4400, or by visiting the [Oregon Attorney General website](#). [↗](#)

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

APPENDIX E – INFORMATION FOR THOSE RESIDING IN OTHER LOCATIONS

[▲Top](#)

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below is information about steps you can take to place a fraud alert or security freeze and check your credit report (where it is available). If you believe you are a victim of fraud or identity theft, you should contact your local law enforcement agency and bank. Please know that contacting us will not expedite any remediation of suspicious activity.

Additionally, you can consult [Europol’s tips and advice](#) [↗](#) on identity theft prevention.

INFORMATION ON OBTAINING A CREDIT REPORT

In some European countries, residents are entitled to view their credit status. For example, in the UK residents can contact either Experian or Equifax to obtain a copy of their credit report, and in Germany residents can contact SCHUFA. Please check whether credit reports are maintained in your jurisdiction and consider whether it would be helpful for you to obtain and review your credit report.

INFORMATION ON IMPLEMENTING A FRAUD ALERT

You may also be able to place a fraud alert on your credit report or with your bank. 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 generally 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.

PLAN A CRUISE	GROUP TRAVEL	ALREADY BOOKED	CUSTOMER SERVICE	CORPORATE	ABOUT CARNIVAL
Today's Deals	Group Shore Excursions	Manage My Cruises	FAQs	World's Leading Cruise Lines ↗	About Us
Search Cruises	Charters, Meetings & Incentives ↗	Shore Excursions	Contact Us	Sustainability ↗	Cruise Ticket Contract
Travel Agent Finder	Themed Cruises ↗	In-Room Gifts & Shopping	Guests with Disabilities	Business Ethics ↗	Passenger Bill Of Rights
Weddings & Occasions		Spa & Salon Services	Early Saver Price Protection Form	Diversity & Inclusion	Safety and Security
Carnival Journeys		Internet Plans	Lowest Price Guarantee Claim Form	Slavery Statement	St. Jude
Gift Cards ↗		Beverage Packages	Great Vacation Guarantee	Investor Relations ↗	
Carnival MasterCard		Organizer Access	Lost and Found ↗	Carnival Foundation ↗	
Financing Powered by Uplift		Carnival HUB App ↗	Post-Cruise Inquiries	Discover OCEAN ↗	
Carnival EasyPay		Fly2Fun			
VIFP Club		Airport Transportation			

Do Not Sell My
Personal
Information

[Press/Media](#) [Legal Notices](#) [Privacy & Cookies](#) [Careers](#) [Travel Partners](#) [Site Map](#)



© 2020 Carnival Corporation.
All rights reserved.

[↗](#) Indicates external site which may or may not meet accessibility guidelines.

*Taxes, fees and port expenses are additional. [View terms and conditions](#)

Investor Relations

News Release

Carnival Corporation & plc Update on Cyber Event

Company issues update to its August 17 announcement

MIAMI, Oct. 13, 2020 /PRNewswire/ -- As earlier disclosed, Carnival Corporation & plc (NYSE/LSE: CCL; NYSE: CUK) detected unauthorized third-party access to portions of the company's information technology systems on August 15, 2020. Information Security at Carnival Corporation acted quickly to shut down the intrusion, restore operations and prevent further unauthorized access. The company also engaged a major cybersecurity firm to investigate the matter and notified law enforcement and appropriate regulators of the event.

While the investigation is ongoing, early indications are that in early August the unauthorized third party gained access to certain personal information relating to some guests, employees and crew for three of the corporation's brands -- Carnival Cruise Line, Holland America Line and Seabourn, as well as casino operations. Working with its cybersecurity consultants, the company took steps to recover its files and has evidence indicating a low likelihood of the data being misused.

The company is working as quickly as possible to identify the guests, employees, crew and other individuals whose personal information may have been impacted. The company expects to complete this process within the next 30 to 60 days and will then send notifications to potentially affected individuals whose current contact information is available to the company. Along with those individual notices, affected individuals will be offered complimentary credit monitoring, as appropriate.

Meanwhile, the company has posted website notices and established a dedicated call center to answer questions regarding the event. When the investigation is complete, callers may confirm whether or not their information was affected.

Additional information about the event is available at www.hollandamerica.com, www.carnival.com, www.seabourn.com, or www.oceanplayersclub.com. The call center is available toll-free in the U.S. at +1. 888.905.0687, 9 a.m. to 9 p.m. Eastern Time (ET), Monday through Friday. Individuals outside the U.S. may email questions to cruisedataevent@cyberscout.com, as well as request that a call center representative respond back by phone.

As part of its ongoing operations, the company is continuing to review security and privacy policies and procedures and implementing changes when needed to enhance information security and privacy controls.

About Carnival Corporation & plc

Carnival Corporation & plc is one of the world's largest leisure travel companies with a portfolio of nine of the world's leading cruise lines. With operations in North America, Australia, Europe and Asia, its portfolio features Carnival Cruise Line, Princess Cruises, Holland America Line, Seabourn, P&O Cruises (Australia), Costa Cruises, AIDA Cruises, P&O Cruises (UK) and Cunard.

🔗 View original content: <http://www.prnewswire.com/news-releases/carnival-corporation--plc-update-on-cyber-event-301151284.html>

SOURCE Carnival Corporation & plc

Roger Frizzell, Carnival Corporation, rfrizzell@carnival.com, (305) 406-7862, Mike Flanagan, LDWW, mike@ldww.co, (727) 452-4538

