Website Notice – Substitute Notice

Carnival Corporation Notice of Data Breach

May 27, 2026

Carnival Corporation values the trust you place in us, and we take the privacy and security of your information very seriously. Unfortunately, a cybersecurity event in April 2026 affected certain personal information for some individuals. We deeply regret this incident and any concern it may cause and have sent notification letters to individuals whose data was impacted.

This notice is intended to provide the same information included in the notification letters to individuals for whom the company has insufficient or out-of-date contact information.

What happened

On April 14, 2026, our IT security team identified unauthorized activity involving an employee's account. An unauthorized actor used social engineering to deceive an employee to gain access to a limited portion of our company's IT system. We acted swiftly to block the unauthorized activity and immediately began working with third party security experts to further strengthen our security and to conduct a thorough investigation. On April 22, 2026, we first determined that the bad actor illegally copied personal information.

What Personal Information was involved

We have been conducting a thorough and time-consuming analysis of the impacted data to determine what personal information it contained and to whom that information belongs. While this analysis is ongoing and the affected data varies by individual, to date, the impacted data is known to include the following personal information: name, address, email address, phone number, date of birth, and government-issued identification number (e.g., driver's license number and passport number).

What we are doing

We are notifying individuals whose personal information was affected via email, as required and where available. We are offering individuals in the U.S. two years of complimentary credit monitoring through its preferred third-party vendor, TransUnion. The notices provide the nature of the information involved and contact details for the dedicated TransUnion call center established to assist with enrollment for eligible individuals and to address any questions related to the incident. Individual notifications were issued starting May 27, 2026.

In addition to the comprehensive security measures our company had in place prior to the incident, we have taken steps to further safeguard our systems, including enhancing our security and monitoring controls. Our company will continue to advance our IT security and data privacy controls to stay ahead of an ever-evolving threat landscape.

What you can do

Together with enrolling in the credit monitoring services being offered to eligible individuals whose data was impacted at no charge, we encourage you to take ongoing data security precautions:

- Remain vigilant against threats of identity theft or fraud and regularly review and monitor account statements and credit histories for any signs of unauthorized transactions or activity.
- If you suspect you are the victim of identity theft or fraud, contact your local police.

For more information

We have established a dedicated call center to answer questions about the incident as well as the TransUnion services that we are offering to you. If you have any questions, please call the TransUnion call center at 1-844-593-8310, from 8 a.m. to 8 p.m. ET Monday through Friday, excluding major U.S. holidays.

Additional information for U.S. residents

U.S. customers 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 +1 (877) 322-8228.

You may contact the U.S. Federal Trade Commission (FTC) for 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.

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.

District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400, oag@dc.gov and www.oag.dc.gov.

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; +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, Maryland 21202; +1 (888) 743-0023 or www.marylandattorneygeneral.gov.

Massachusetts residents: Under Massachusetts law, you have the right to obtain any police report filed in connection with the cybersecurity event. 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 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 https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-march-2026.pdf or www.ftc.gov.

New York residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341; +1 (800)-771-7755 or www.ag.ny.gov.

Oregon residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 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.

For Arizona, California, Iowa, Montana, Washington and West Virginia 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 bureaus directly to obtain such additional report(s).

FAQs

1. **What happened?**
   On April 14, 2026, the Company's IT security team identified unauthorized activity involving an employee's account. An unauthorized actor used social engineering to deceive an employee to gain access to a limited portion of the Company's IT system. The Company acted swiftly to block the unauthorized activity and immediately began working with third party security experts to further strengthen our security and to conduct a thorough investigation. On April 22, 2026, the Company first determined that the bad actor illegally copied personal information.

   In addition to the enterprise-wide security measures the Company had in place prior to the incident, we have taken steps to further safeguard our systems, including enhancing our security and monitoring controls. The Company will continue to advance its IT security and data privacy controls to stay ahead of an ever-evolving threat landscape.

2. **What type of data was stolen?**
   The Company has been analyzing the impacted data and after determining it contained personal information, we have been working to identify who that information belongs to. This analysis has been time consuming. To date, the impacted data is known to include the following personal information: name, address, email address, phone number, date of birth, and government-issued identification number (e.g., driver's license number and passport number).

3. **How many individuals were affected by this incident?**
   Starting on or about May 27, 2026, we began notifying individuals whose personal information was affected via email, as required and where available. This notice is intended to provide the same information included in the notification letters to individuals for whom the company has insufficient or out-of-date contact information.

4. **When and how were notifications sent?**
   We began sending email notifications to individuals whose personal information was impacted starting on or about May 27, 2026. If you received an email notification related to this incident, please read the notice carefully to learn what happened and what we are doing.

5. **Has the event been resolved/contained?**
   We are not aware of any unauthorized activity since we stopped the attack on April 14.

6. **Does the Company store customer payment information or collect customer data?**
   You may find our privacy policy and the information we collect, here (CarnivalCorp.com/privacy-notice).

7. **Why am I just finding out about this?**
   We understand this process can feel slow, and we appreciate your patience. Complex incidents like this take time and careful investigation to understand what information was affected and who it belongs to, and then to ensure notifications are handled accurately. After identifying and stopping the incident, our focus shifted immediately to investigating it fully and communicating with all impacted parties as soon as we could.

8. **Has law enforcement been notified?**
   Yes, law enforcement was notified.

9. **What actions are you taking to better secure the Company's network in response to this event?**
   Prior to the incident, the Company had a number of security measures in place but has taken further steps to deploy additional safeguards onto our systems, including implementing enhanced security and monitoring controls. We remain committed to ongoing information security reviews to strengthen our security and privacy programs and controls.

10. **Should I request a fraud alert from the credit reporting agencies? What is a fraud alert?**
That is an individual decision. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. There are also two types of fraud alerts that 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, with 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 calling the toll-free fraud number of any of the three national credit reporting agencies as follows:

Equifax: 1-888-766-0008, https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian: 1-888-397-3742, https://www.experian.com/fraud/center.html
TransUnion: 1-800-680-7289, https://www.transunion.com/fraud-victim-resource/place-fraud-alert

11. **Should I freeze my credit? What is a credit or security freeze?**
That is an individual decision. You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

12. **How does someone obtain a free copy of his or her credit report?**
You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting companies. To order your annual free report, please visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or directly contact the three nationwide credit reporting companies:

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 2002	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	1-800-916-8800