**Website Substitute Notice**

**Substitute Notice**

The Port of Seattle (the “Port”) today announced that notification letters have been mailed to individuals whose data was impacted in the August 2024 cyberattack.

This website notice is intended to provide the same information included in the notification letters to individuals for whom the Port has insufficient or out-of-date contact information. The Port previously launched [a website](https://www.portseattle.org/news/port-cyberattack-archive) to report the incident publicly August 24, 2024.

**Notice of Data Breach**

**What happened**

On August 24, 2024, the Port identified system outages consistent with a cyberattack. The Port promptly initiated its incident response processes. Our teams isolated critical systems, took certain systems offline, and worked with third-party and federal partners to safely restore and test our systems.

Importantly, at no point did this incident affect the ability to safely travel to or from Seattle-Tacoma International Airport or safely use the Port’s maritime facilities. The proprietary systems of our major airline and cruise partners were not affected, nor were the systems of our federal partners like the Federal Aviation Administration, Transportation Security Administration, and U.S. Customs and Border Protection.

An investigation assisted by cybersecurity and technology experts was initiated to investigate what happened and what data may have been impacted. The impacted data was then reviewed to determine who needed to be notified and the contact information for doing so. The Port also notified law enforcement and worked to add further protections to harden its systems.

**What Personal Information Was Involved**

We determined that around August 24, 2024, the threat actors accessed and downloaded some personal information from the Port networks, mostly for current and former Port and other airport employees and contractors. Within these downloaded files, the Port identified the following personal information that may have been involved for impacted individuals: name, date of birth, full or partial Social Security number, government issued identification number, health information, and financial or payment account number.

**What We Are Doing**

Prior to the incident, the Port had a number of security measures in place. As part of the recovery process, the Port implemented additional technical and administrative security controls to further enhance the security of our systems and data.

The Port is notifying individuals whose personal information was affected via mail where available. The Port began sending the first rounds of individual notifications on April 3, 2025. These notifications include an offer of one year of comprehensive credit monitoring and identity theft protection services. Additionally, the notices provide detailed information of these services, along with instructions for registration and contact details for our dedicated call center established to assist with enrollment and to address any inquiries related to the incident.

**What you can do**

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. If you provided your personal information to the Port prior to August 24, 2024 and you do not receive a notification by April 10, 2025, please call 1-833-998-8263.

**For more information:**

A dedicated call center is also being set up to answer your questions about this incident. You may call it toll free at 1-833-998-8263, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

**Additional Information for US Residents**

**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](http://www.annualcreditreport.com/) or call toll‑free (877) 322‑8228.

**INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE**

You can 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:

|  |  |  |
| --- | --- | --- |
| Equifax:  Consumer Fraud Division  P.O. Box 740256  Atlanta, GA 30374  (800) 525-6285  [www.equifax.com](http://www.equifax.com) | Experian:  Credit Fraud Center  P.O. Box 9554  Allen, TX 75013  (888) 397-3742  [www.experian.com](file:///C:\Users\DJC7\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\H45J579Y\www.experian.com) | TransUnion:  TransUnion LLC  P.O. Box 2000  Chester, PA 19022-2000  (800) 680-7289  [www.transunion.com](http://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](http://www.consumer.gov/idtheft).