

Port of Seattle
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Port
of Seattle

[REDACTED]
[REDACTED]
[REDACTED] WA [REDACTED]



April 3, 2025

Re: Notice of Data Breach

[REDACTED]:

We are writing to inform you that some of your personal information was impacted when Port of Seattle (the “Port”) was the victim of a cybersecurity attack. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.

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 a 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 around August 24, 2024 that 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 about you: [REDACTED]

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.

000010102G0500

P

The Port is offering you a complimentary twelve (12)-month membership to TransUnion's credit monitoring and identity theft protection services. We are also 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. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Please see [Attachment A](#) below for additional details regarding these services. **You must enroll by July 2, 2025 to receive these services.**

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. You can also enroll in the TransUnion service being offered to you. Additional information about how to protect your identity and personal data is contained in [Attachment B](#) below.

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.

Sincerely,

Port of Seattle Information Security

Attachment A - Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 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.

Attachment B - More Information about Identity Protection

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



00001020280000

P

